

SENATE



SÉNAT

First Session
Forty-second Parliament, 2015-16-17-18

Première session de la
quarante-deuxième législature, 2015-2016-2017-2018

*Proceedings of the Standing
Senate Committee on*

*Délibérations du Comité
sénatorial permanent des*

BANKING, TRADE AND COMMERCE

BANQUES ET DU COMMERCE

Chair:

The Honourable DOUGLAS BLACK

Président :

L'honorable DOUGLAS BLACK

Wednesday, February 28, 2018
Thursday, March 1, 2018

Le mercredi 28 février 2018
Le jeudi 1^{er} mars 2018

Issue No. 35

Fascicule n° 35

Fifth and sixth meetings:

Study and report on issues and
concerns pertaining to cyber security
and cyber fraud

and

Sixteenth meeting:

Study on the present state of the domestic
and international financial system

WITNESSES:

(See back cover)

Cinquième et sixième réunions :

Étudier, pour en faire rapport, les questions
et préoccupations relatives à la cybersécurité
et à la cyberfraude

et

Seizième réunion :

Étude sur la situation actuelle du régime
financier canadien et international

TÉMOINS :

(Voir à l'endos)

STANDING SENATE COMMITTEE ON
BANKING, TRADE AND COMMERCE

The Honourable Douglas Black, *Chair*

The Honourable Carolyn Stewart Olsen, *Deputy Chair*
and

The Honourable Senators:

Dagenais	* Smith
Day	(or Martin)
* Day	Tannas
(or Mercer)	Tkachuk
* Harder, P.C.	Unger
(or Bellemare)	Wallin
(or Mitchell)	Wetston
Marwah	* Woo
Ringuette	(or Saint-Germain)

*Ex officio members
(Quorum 4)

Change in membership of the committee:

Pursuant to rule 12-5 and to the order of the Senate of November 7, 2017, membership of the committee was amended as follows:

The Honourable Senator Tkachuk replaced the Honourable Senator Neufeld (*February 15, 2018*).

COMITÉ SÉNATORIAL PERMANENT DES
BANQUES ET DU COMMERCE

Président : L'honorable Douglas Black

Vice-présidente : L'honorable Carolyn Stewart Olsen
et

Les honorables sénateurs :

Dagenais	* Smith
Day	(ou Martin)
* Day	Tannas
(ou Mercer)	Tkachuk
* Harder, C.P.	Unger
(ou Bellemare)	Wallin
(ou Mitchell)	Wetston
Marwah	* Woo
Ringuette	(ou Saint-Germain)

* Membres d'office
(Quorum 4)

Modification de la composition du comité :

Conformément à l'article 12-5 du Règlement et à l'ordre adopté par le Sénat le 7 novembre 2017, la liste des membres du comité est modifiée, ainsi qu'il suit :

L'honorable sénateur Tkachuk a remplacé l'honorable sénateur Neufeld (*le 15 février 2018*).

MINUTES OF PROCEEDINGS

OTTAWA, Wednesday, February 28, 2018
(89)

[English]

The Standing Senate Committee on Banking, Trade and Commerce met this day at 4:30 p.m., in room 9, Victoria Building, the chair, the Honourable Douglas Black, presiding.

Members of the committee present: The Honourable Senators Black (*Alberta*), Dagenais, Marwah, Stewart Olsen, Tannas and Wetston (6).

In attendance: Chantal Cardinal, Procedural Clerk, Committees Directorate; Adriane Yong, Analyst, Parliamentary Information and Research Services, Library of Parliament.

Also present: The official reporters of the Senate.

Pursuant to the order of reference adopted by the Senate on Tuesday, October 17, 2017, the committee continued its study on issues and concerns pertaining to cyber security and cyber fraud. (*For the complete text of the order of reference, see proceedings of the committee, Issue No. 26.*)

WITNESSES:*Bank of Canada:*

Ron Morrow, Managing Director, Financial Stability Department.

Department of Finance Canada:

Annette Ryan, Associate Assistant Deputy Minister, Financial Sector Policy Branch.

Office of the Superintendent of Financial Institutions Canada:

Judy Cameron, Senior Director, Legislation, Approvals and Strategic Policy;

Theresa Hinz, Director, Approvals and Precedents.

Payments Canada:

Justin Ferrabee, Chief Operating Officer;

Martin Kyle, Chief Information Security Officer.

The chair made a statement.

Ms. Ryan, Mr. Morrow and Ms. Cameron each made a statement and, together with Ms. Hinz, answered questions.

At 5:29 p.m., the committee suspended.

At 5:32 p.m., the committee resumed.

The chair made a statement.

Mr. Ferrabee made a statement and, together with Mr. Kyle, answered questions.

PROCÈS-VERBAUX

OTTAWA, le mercredi 28 février 2018
(89)

[Français]

Le Comité sénatorial permanent des banques et du commerce se réunit aujourd'hui, à 16 h 30, dans la pièce 9 de l'édifice Victoria sous la présidence de l'honorable Douglas Black (*président*).

Membres du comité présents : Les honorables sénateurs Black (*Alberta*), Dagenais, Marwah, Stewart Olsen, Tannas et Wetston (6).

Également présente : Chantal Cardinal, greffière à la procédure, Direction des comités; Adriane Yong, analyste, Service d'information et de recherche parlementaires, Bibliothèque du Parlement.

Aussi présents : Les sténographes officiels du Sénat.

Conformément à l'ordre de renvoi adopté par le Sénat le mardi 17 octobre 2017, le comité entreprend son étude sur les questions et préoccupations relatives à la cybersécurité et à la cyberfraude. (*Le texte intégral de l'ordre de renvoi figure au fascicule n° 26 des délibérations du comité.*)

TÉMOINS :*Banque du Canada :*

Ron Morrow, directeur général, Département de la Stabilité financière.

Ministère des Finances Canada :

Annette Ryan, sous-ministre adjointe déléguée, Direction de la politique du secteur financier.

Bureau du surintendant des institutions financières Canada :

Judy Cameron, directrice principale, Législation, approbations et politique stratégique;

Theresa Hinz, directrice, Approbations et précédents.

Paiements Canada :

Justin Ferrabee, chef des opérations;

Martin Kyle, dirigeant principal de la sécurité de l'information.

Le président fait une déclaration.

Mme. Ryan, M. Morrow et Mme Cameron font chacun une déclaration et, avec Mme Hinz, répondent aux questions.

À 17 h 29, la séance est suspendue.

À 17 h 32, la séance reprend.

Le président fait une déclaration.

M. Ferrabee fait une déclaration et, avec M. Kyle, répond aux questions.

At 6:05 p.m., the committee adjourned to the call of the chair.

ATTEST:

OTTAWA, Thursday, March 1, 2018
(90)

[English]

The Standing Senate Committee on Banking, Trade and Commerce met this day at 10:30 a.m., in room 9, Victoria Building, the chair, the Honourable Douglas Black, presiding.

Members of the committee present: The Honourable Senators Black (*Alberta*), Dagenais, Stewart Olsen, Tannas, Tkachuk and Wetston (6).

In attendance: Chantal Cardinal, Procedural Clerk, Committees Directorate; Adriane Yong and Brett Stuckey, Analysts, Parliamentary Information and Research Services, Library of Parliament.

Also present: The official reporters of the Senate.

Pursuant to the order of reference adopted by the Senate on Tuesday, October 17, 2017, the committee continued its study on issues and concerns pertaining to cyber security and cyber fraud. (*For the complete text of the order of reference, see proceedings of the committee, Issue No. 26.*)

WITNESSES:

The Canadian Chamber of Commerce:

Scott Smith, Director, Intellectual Property and Innovation Policy.

Canadian Cyber Threat Exchange:

Robert W. Gordon, Executive Director.

MasterCard:

Ron Green, Chief Security Officer.

The chair made a statement.

Messrs. Gordon, Smith and Green each made a statement and, together, answered questions.

At 11:29 a.m., the committee suspended.

At 11:32 a.m., the committee resumed.

Pursuant to the order of reference adopted by the Senate on Wednesday, January 27, 2016, the committee continued its study on the present state of the domestic and international financial system. (*For complete text of the order of reference, see proceedings of the committee, Issue No. 2.*)

À 18 h 5, la séance est levée jusqu'à nouvelle convocation de la présidence.

ATTESTÉ :

OTTAWA, le jeudi 1^{er} mars 2018
(90)

[Français]

Le Comité sénatorial permanent des banques et du commerce se réunit aujourd'hui, à 10 h 30, dans la pièce 9 de l'édifice Victoria sous la présidence de l'honorable Douglas Black (*président*).

Membres du comité présents : Les honorables sénateurs Black (*Alberta*), Dagenais, Stewart Olsen, Tannas, Tkachuk et Wetston (6).

Également présents : Chantal Cardinal, greffière à la procédure, Direction des comités; Adriane Yong et Brett Stuckey, analystes, Service d'information et de recherche parlementaires, Bibliothèque du Parlement.

Aussi présents : Les sténographes officiels du Sénat.

Conformément à l'ordre de renvoi adopté par le Sénat le mardi 17 octobre 2017, le comité entreprend son étude sur les questions et préoccupations relatives à la cybersécurité et à la cyberfraude. (*Le texte intégral de l'ordre de renvoi figure au fascicule n° 26 des délibérations du comité.*)

TÉMOINS :

Chambre de commerce du Canada :

Scott Smith, directeur, Propriété intellectuelle et politique d'innovation.

Échange canadien de menaces cybernétiques :

Robert W. Gordon, directeur général.

MasterCard :

Ron Green, chef de la sécurité.

Le président fait une déclaration.

MM. Gordon, Smith et Green font chacun une déclaration et répondent aux questions.

À 11 h 29, la séance est suspendue.

À 11 h 32, la séance reprend.

Conformément à l'ordre de renvoi adopté par le Sénat le mercredi 27 janvier 2016, le comité poursuit son étude sur la situation actuelle du régime financier canadien et international. (*Le texte intégral de l'ordre de renvoi figure au fascicule n° 2 des délibérations du comité.*)

*WITNESSES:**International Monetary Fund:*

Cheng Hoon Lim, Assistant Director and Mission Chief for Canada, Western Hemisphere Department (by video conference);

Troy Matheson, Senior Economist (by video conference);

Kotaro Ishi, Senior Economist (by video conference).

The chair made a statement.

Ms. Lim made a statement and, together with Mr. Matheson and Mr. Ishi, answered questions.

At 12:07 p.m., the committee adjourned to the call of the chair.

*ATTEST:**TÉMOINS :**Fonds monétaire international :*

Cheng Hoon Lim, sous-directrice et chef de mission pour le Canada, Département hémisphère occidental (par vidéoconférence);

Troy Matheson, économiste principal (par vidéoconférence);

Kotaro Ishi, économiste principal (par vidéoconférence).

Le président fait une déclaration.

Mme. Lim fait une déclaration et, avec MM. Matheson et Ishi, répond aux questions.

À 12 h 7, la séance est levée jusqu'à nouvelle convocation de la présidence.

ATTESTÉ :

Le greffier du comité par intérim,

Adam Thompson

Acting Clerk of the Committee

EVIDENCE

OTTAWA, Wednesday, February 28, 2018

The Standing Senate Committee on Banking, Trade and Commerce met this day at 4:30 p.m. to study and report on issues and concerns pertaining to cyber security and cyber fraud.

Senator Douglas Black (*Chair*) in the chair.

[*English*]

The Chair: Good afternoon and welcome colleagues and members of the general public who may be watching this on the Web. Today, you are before the Standing Senate Committee on Banking, Trade and Commerce, and we welcome you. My name is the Doug Black and I am the chair of this committee. Other senators will be joining us. I apologize, but we've just come from a vote in the Senate. I'm going to ask the senators who are here to introduce themselves.

Senator Marwah: Sabi Marwah, Ontario.

Senator Tannas: Scott Tannas, Alberta.

[*Translation*]

Senator Dagenais: Jean-Guy Dagenais from Quebec.

[*English*]

Senator Stewart Olsen: Carolyn Stewart Olsen, New Brunswick.

Senator Wetston: Howard Wetston, Ontario.

The Chair: Thank you very much for being here. Since we're starting a little bit late and I don't want to cramp the valuable information we will hear from you, we will extend this panel until 5:30 if we should need that.

Today we resume our study on issues and concerns pertaining to cybersecurity and cyberfraud. This study includes cyberthreats to Canada's financial and commercial sectors; identity theft; privacy breach and other fraudulent activities targeting Canadian consumers and small business; the current state of cybersecurity technologies and cybersecurity measures and regulations in Canada and abroad.

I am pleased to welcome Annette Ryan, Associate Assistant Deputy Minister, Financial Sector Policy Branch, Department of Finance Canada; Ron Morrow, Managing Director, Financial Stability Department, Bank of Canada; Judy Cameron, Senior Director, Legislation, Approvals and Strategic Policy, Office of the Superintendent of Financial Institutions Canada; and Theresa

TÉMOIGNAGES

OTTAWA, le mercredi 28 février 2018

Le Comité sénatorial permanent des banques et du commerce se réunit aujourd'hui, à 16 h 30, afin d'étudier, pour en faire rapport, les questions et préoccupations relatives à la cybersécurité et à la cyberfraude.

Le sénateur Douglas Black (*président*) occupe le fauteuil.

[*Traduction*]

Le président : Bonjour et bienvenue à mes collègues et aux membres du public qui nous regardent peut-être sur le Web. Aujourd'hui, vous êtes devant le Comité sénatorial permanent des banques et du commerce. Nous vous souhaitons la bienvenue. Je m'appelle Doug Black et je suis président du comité. D'autres sénateurs se joindront à nous. Je m'excuse, mais nous venons de terminer un vote au Sénat. J'invite les sénateurs qui sont ici à se présenter.

Le sénateur Marwah : Sabi Marwah, de l'Ontario.

Le sénateur Tannas : Scott Tannas, de l'Alberta.

[*Français*]

Le sénateur Dagenais : Jean-Guy Dagenais, du Québec.

[*Traduction*]

La sénatrice Stewart Olsen : Carolyn Stewart Olsen, du Nouveau-Brunswick.

Le sénateur Wetston : Howard Wetston, de l'Ontario.

Le président : Je vous remercie beaucoup d'être ici. Puisque nous commençons avec un peu de retard et que je ne veux pas nous priver des renseignements importants que vous nous communiquerez, la réunion sera prolongée jusqu'à 17 h 30, au besoin.

Aujourd'hui, nous reprenons notre étude sur les questions et préoccupations relatives à la cybersécurité et à la cyberfraude, y compris les cybermenaces pesant sur le secteur financier et commercial au Canada; le vol d'identité, l'atteinte à la vie privée et les autres activités frauduleuses ciblant les consommateurs canadiens et les petites entreprises; l'état actuel des technologies de cybersécurité; et les mesures et les règlements liés à la cybersécurité au Canada et à l'étranger.

Je suis heureux de souhaiter la bienvenue à Annette Ryan, sous-ministre adjointe déléguée, Direction de la politique du secteur financier, ministère des Finances Canada, à Ron Morrow, directeur général, Département de la Stabilité financière, Banque du Canada, à Judy Cameron, directrice principale, Législation, approbations et politique stratégique, Bureau du surintendant des institutions financières Canada, et à Theresa Hinz, directrice,

Hinz, Director, Approvals and Precedents from the Office of the Superintendent of Financial Institutions Canada.

I'm going to ask for a five-minute opening presentations and then the senators will have questions.

Annette Ryan, Associate Assistant Deputy Minister, Financial Sector Policy Branch, Department of Finance Canada: Thank you for inviting my colleagues and I to speak to you today on the important topic of cybersecurity.

[Translation]

My name is Annette Ryan. I am Associate Assistant Deputy Minister of the Financial Sector Policy Branch at the Department of Finance. The Financial Sector Policy Branch is responsible for providing policy advice on Canada's financial sector, including the framework for federally regulated financial institutions, financial systems under federal jurisdiction, federal borrowing and investments, financial services trade, and capital markets matters. The branch works closely with a number of federal financial sector agencies, including the Bank of Canada and the Office of the Superintendent of Financial Institutions, which are both represented here today.

Cybersecurity is top of mind for both the private sector and the federal government. In recent years, this topic has become increasingly important at all levels of government and internationally.

[English]

Rapid changes in technology, many eagerly adopted by Canadians, are revolutionizing how the financial sector delivers its services and interacts with its customers. Before delving further into the risks entailed by technology, it is worth highlighting that financial technology innovations also bring many opportunities for business and consumers, including the convenience of performing financial transactions any time and anywhere.

Of course, along with these opportunities come major risks. As Canadians increasingly engage with financial service providers in an online and mobile environment, the risks increase in turn.

In the financial sector, cyberattacks threaten to disrupt the services provided by financial institutions, compromise the privacy of consumer information and bring about a reputational risk to financial institutions. Cyberattacks have the potential to

Approbations et précédents, Bureau du surintendant des institutions financières Canada.

Je vous demande de donner vos présentations préliminaires de cinq minutes et ensuite les sénateurs vous poseront des questions.

Annette Ryan, sous-ministre adjointe déléguée, Direction de la politique du secteur financier, ministère des Finances Canada : Je vous remercie d'avoir invité mes collègues et moi à parler aujourd'hui sur cet important sujet qu'est la cybersécurité.

[Français]

Je m'appelle Annette Ryan. Je suis sous-ministre adjointe déléguée à la Direction de la politique du secteur financier du ministère des Finances. La Direction de la politique du secteur financier est responsable de fournir des conseils stratégiques sur le secteur financier au Canada, notamment le cadre des institutions financières sous réglementation fédérale, les systèmes financiers de compétence fédérale, les emprunts et les investissements fédéraux, le commerce des services financiers, ainsi que les questions liées aux marchés de capitaux. La Direction collabore étroitement avec un certain nombre d'organismes fédéraux du secteur financier, y compris la Banque du Canada et le Bureau du surintendant des institutions financières, dont des représentants sont ici présents.

La cybersécurité est un enjeu de premier plan, autant pour le secteur privé que pour le gouvernement fédéral. Au cours des dernières années, ce sujet a pris de plus en plus d'importance pour tous les ordres de gouvernement et à l'échelle internationale.

[Traduction]

Les changements rapides dans le domaine de la technologie, dont bon nombre sont adoptés avec empressement par les Canadiens, révolutionnent la façon dont le secteur financier offre ses services et interagit avec ses clients. Avant de se pencher davantage sur les risques que comporte la technologie, il convient de souligner que les innovations technologiques dans le secteur financier comportent également de nombreuses possibilités pour les entreprises et les consommateurs, notamment la commodité d'effectuer des opérations financières à tout moment et partout.

Bien entendu, des risques majeurs accompagnent ces possibilités. Comme les Canadiens collaborent de plus en plus avec les fournisseurs de services financiers dans un environnement en ligne et mobile, les risques augmentent proportionnellement.

Dans le secteur financier, les cyberattaques menacent d'interrompre les services fournis par les institutions financières, de mettre en péril la confidentialité des renseignements du client et d'entraîner un risque à la réputation des institutions

disrupt financial services that are crucial to both national and international financial systems and so endanger financial stability. From a government regulations perspective, there are also important risks that need to be properly accounted for. In line with the Minister of Finance's responsibility for the overall health of the Canadian financial system, we approach cybersecurity discussions from a financial stability angle.

The growing global reach of financial service providers, be they major financial institutions or an Internet-based money service provider, means one weak link in the chain can import risk into the broader financial system if not well governed and coordinated. As you've learned from previous witnesses, cyber-threats and the vulnerabilities which they exploit emerge and evolve constantly. As such, increasing the resiliency of the financial sector and reinforcing its recovery processes require coordinated action at all levels.

[Translation]

Finance Canada plays an active role in facilitating the coordination of multiple actors involved in discussions on cybersecurity within the financial sector, be it the financial institutions themselves, other federal and provincial government agencies and international partners. We maintain an ongoing dialogue with federally regulated financial institutions. It is important for us to hear firsthand what their key concerns are in relation to cybersecurity and what kind of actions the government may take to remediate them.

We act as a facilitator between the financial sector and other departments that have program responsibilities in relation to cybersecurity, notably, Public Safety, which leads on broader Government of Canada initiatives for cybersecurity, including Canada's cybersecurity strategy.

[English]

I know you have heard these themes from past testimonies, and that brings us to yesterday's budget as we have heard similar representations from these sources.

Budget 2018 announced significant investments — over half a billion dollars over five years — to launch a comprehensive national cybersecurity strategy to bolster the safety of Canadians and Canadian businesses online.

financières. Les cyberattaques peuvent éventuellement interrompre des services financiers qui sont essentiels pour les systèmes financiers nationaux et internationaux et ainsi compromettre la stabilité financière. Du point de vue de la réglementation du gouvernement, ce sont des risques importants qui doivent être pris en compte adéquatement. Conformément à la responsabilité du ministre des Finances concernant la santé générale du système financier canadien, nous abordons les discussions sur la cybersécurité sous l'angle de la stabilité financière.

La portée mondiale croissante des fournisseurs de services financiers — qu'il s'agisse d'importantes institutions financières ou de fournisseurs de services de transfert d'argent sur Internet — signifie qu'un maillon faible de la chaîne peut entraîner un risque au système financier dans son ensemble, si ce dernier n'est pas bien gouverné et coordonné. Comme les témoins précédents vous l'ont appris, les cybermenaces et les vulnérabilités qu'elles exploitent continuent de se produire et d'évoluer. Une augmentation de la résilience du secteur financier et un renforcement des processus de rétablissement nécessitent donc des mesures coordonnées à tous les niveaux.

[Français]

Le ministère des Finances du Canada joue un rôle actif en favorisant la coordination de plusieurs acteurs qui participent aux discussions sur la cybersécurité dans le secteur financier, qu'il s'agisse des institutions financières elles-mêmes, d'autres organismes gouvernementaux fédéraux et provinciaux ou de partenaires internationaux. Nous maintenons un dialogue continu avec les représentants d'institutions financières sous réglementation fédérale. Nous croyons qu'il est important de les entendre parler directement de leurs préoccupations relatives à la cybersécurité et de connaître les mesures que le gouvernement peut prendre pour les régler.

Nous jouons un rôle de facilitateur entre le secteur financier et les autres ministères qui ont des responsabilités en matière de programmes relativement à la cybersécurité, notamment la Sécurité publique, qui mène les initiatives plus élargies du gouvernement fédéral en matière de cybersécurité, y compris la Stratégie de cybersécurité du Canada.

[Traduction]

Je sais que ces thèmes ont été discutés lors de témoignages précédents, ce qui nous amène au budget d'hier puisque nous avons entendu des représentations semblables de ces sources.

Le budget de 2018 annonce d'importants investissements — plus d'un demi-milliard de dollars pour les cinq prochaines années — pour lancer une Stratégie nationale de cybersécurité exhaustive qui renforcera la sécurité des Canadiens et des entreprises canadiennes en ligne.

The centrepiece of the government's new plan is the creation of the Canadian Centre for Cyber Security, establishing a single source of federal cybersecurity advice and expertise for key partners, including the private sector. The new strategy will also see the establishment of national cybercrime coordination unit, which creates a national reporting mechanism for Canadians to report cybercrime to law enforcement and gives them new resources to investigate cybercrimes and prosecute cybercriminals.

The national cybersecurity strategy will enhance Canada's cybersecurity resilience, allow us to respond more quickly to cyberattacks and will raise the cybersecurity bar for all Canadians.

We also believe we can learn from other countries' experiences and we participate actively at the international level, notably through the Financial Stability Board, the G20 and G7. To this end, Finance Canada, the Bank of Canada and Office of the Superintendent of Financial Institutions Canada have been active members of the G7 Cyber Expert Group, which reports to the G7 finance ministers and central bank governors. This group has published documents that identify best practices G7 members can follow and provides guideposts to other countries seeking to improve their security. The group is advancing work to identify and manage third party risks and to promote timely international coordination of response and recovery efforts in the event of a successful material cyberattack in the financial sector.

As Canada has assumed the G7 presidency in 2018, we are leading further progress in these specific areas of coordination. We firmly believe reinforcing security and resilience in cyberspace requires close cooperation and collaboration nationally and internationally from the various actors touched by cybersecurity. Importantly, joint private and public sector roles should work in concert and we are very focused on continuing to work with industry, now within the national cybersecurity strategy, which was announced yesterday. We look forward the hearing the perspective of other witnesses called to your committee and, in particular, the insights of the committee in respect of the financial sector.

Ron Morrow, Managing Director, Financial Stability Department, Bank of Canada: Good afternoon, Mr. Chair and committee members. Thank you for the invitation to speak to you on this timely and important topic.

Au cœur de ce nouveau plan du gouvernement se trouve la création du Centre canadien pour la cybersécurité, qui permettra d'établir une source centralisée qui offrira conseils et expertise en matière de cybersécurité à nos partenaires clés, y compris le secteur privé. La nouvelle stratégie mènera également à la création de l'Unité nationale de coordination de la lutte contre la cybercriminalité qui créera un mécanisme national permettant aux Canadiens de rapporter les cybercrimes aux autorités responsables de l'application de la loi et qui leur donne de nouvelles ressources pour mener des enquêtes sur les cybercrimes et poursuivre les cybercriminels en justice.

La Stratégie nationale de cybersécurité contribuera à améliorer la résilience du Canada en matière de cybersécurité, nous positionnera pour réagir plus vite aux cyberattaques et rehaussera le niveau de cybersécurité pour tous les Canadiens.

Nous croyons également que nous pouvons apprendre de l'expérience des autres pays et nous participons activement à des initiatives à l'échelle internationale, notamment au sein du Conseil de stabilité financière, du G20 et du G7. Dans le même ordre d'idées, le ministère des Finances Canada, la Banque du Canada et le Bureau du surintendant des institutions financières ont été des membres actifs du Groupe d'experts cybernétiques du G7, qui relève des ministres des Finances du G7 et des gouverneurs des banques centrales. Le groupe a publié des documents qui énumèrent des pratiques exemplaires que des membres du G7 peuvent adopter et fournissent des balises aux autres pays qui cherchent à améliorer leur sécurité. Le groupe fait progresser les travaux visant à identifier et à gérer les risques des tiers et à promouvoir une coordination internationale rapide des efforts d'intervention et de rétablissement dans l'éventualité d'une attaque cybernétique importante dans le secteur financier.

Comme le Canada a assuré la présidence du G7 en 2018, nous dirigeons des progrès supplémentaires dans ces domaines de coordination précis. Nous croyons fermement que le renforcement de la sécurité et de la résilience dans le cyberspace nécessite une coopération et une collaboration étroite, sur le plan national et international, des divers acteurs responsables de la cybersécurité. Plus important encore, les personnes qui assument des rôles conjoints dans le secteur privé et le secteur public devraient travailler de concert, et nous voulons fortement continuer de travailler avec l'industrie, conformément à la Stratégie nationale de cybersécurité qui a été annoncée hier. Nous attendons avec intérêt de connaître les points de vue des autres témoins convoqués devant votre comité et, en particulier, les réflexions du comité à l'égard du secteur financier.

Ron Morrow, directeur général, Département de la Stabilité financière, Banque du Canada : Monsieur le président, distingués membres du comité, bonjour. Je vous remercie de m'avoir invité à vous parler aujourd'hui d'un important sujet d'actualité.

[Translation]

Let me start with a brief description of the role the Bank of Canada plays in the Canadian financial system. Our mandate is to foster the stability and efficiency of the Canada's financial system. We do this by providing central banking services, including various mechanisms for providing liquidity to the financial system; overseeing key Canadian financial market infrastructures; conducting and publishing analyses and research; and helping to develop and implement policy.

As the scope and seriousness of cyber-threats has increased, the bank has devoted more and more time and attention to the financial stability concerns they pose. That is why we consider such threats an important vulnerability, as we noted last November in our Financial System Review.

[English]

We consider cyber risks to be a structural vulnerability because they reflect structural features, such as the increase in use of information technology to deliver financial services. Complex information technology platforms have allowed the financial sector to deliver services to clients more efficiently. However, they have also created increased opportunities for a successful cyberattack.

The high degree of interconnectedness between institutions means a single attack against a financial institution could spread to the broader financial system. As a result, cyber-threats have become a key vulnerability that both financial system participants and regulators will have to confront for a long time to come.

[Translation]

So, how is the Bank of Canada helping to mitigate this vulnerability and ensure the ongoing stability of the Canadian financial system? It has identified three priorities: first, ensuring the financial market infrastructures we oversee are taking appropriate steps to mitigate cyber-threats; second, collaborating with financial system participants to support collective actions to improve the resilience of the financial system as a whole; and third, investing to ensure that the bank itself is resilient to cyber-threats.

[English]

I will give the committee a bit more detail on the initiatives we are taking in each of these three areas, but first I wanted to offer a brief background on financial market infrastructures, or FMIs,

[Français]

Si vous me le permettez, je commencerai par présenter brièvement le rôle de la Banque du Canada au sein du système financier canadien. La banque a pour mandat de promouvoir la stabilité et l'efficacité du système financier canadien. À cette fin, elle offre des services de banque centrale, dont plusieurs mécanismes lui permettent de fournir des liquidités au système financier. Elle assure la surveillance des principales infrastructures canadiennes des marchés financiers. Elle effectue et publie des analyses et des recherches, et elle contribue à l'élaboration et à la mise en œuvre des politiques publiques.

L'ampleur et la gravité des cybermenaces s'étant accrues, la banque accorde de plus en plus de temps et d'attention aux risques que ces menaces font peser sur la stabilité financière. C'est pourquoi nous les considérons comme une vulnérabilité, comme nous l'avons mentionné dans notre Revue du système financier en novembre dernier.

[Traduction]

Nous considérons les cyberrisques comme une vulnérabilité structurelle parce qu'ils sont le reflet de réalités structurelles, comme un recours croissant aux technologies de l'information pour offrir des services financiers. Des plateformes informatiques complexes ont permis au secteur financier de servir les clients plus efficacement. Cependant, elles ont également créé davantage d'occasions de mener des cyberattaques réussies.

Le degré élevé d'interconnexion implique qu'une seule attaque contre une institution financière pourrait se propager au système en entier. Par conséquent, les cybermenaces sont devenues une des grandes vulnérabilités que les participants au système financier et les autorités de réglementation devront prendre en considération pendant encore longtemps.

[Français]

Cela étant dit, comment la banque contribue-t-elle à atténuer cette vulnérabilité et à préserver la stabilité du système financier canadien? Elle a dégagé trois priorités à cet égard : premièrement, s'assurer que les infrastructures des marchés financiers soumises à sa surveillance prennent les bonnes mesures pour atténuer les cybermenaces; deuxièmement, appuyer les actions concertées destinées à accroître la résilience du système financier dans son ensemble en collaboration avec les participants au système financier; troisièmement, investir et tout mettre en œuvre pour s'assurer que la Banque du Canada peut elle-même résister aux cybermenaces.

[Traduction]

Je donnerai au comité un peu plus de précisions sur les initiatives que nous prenons dans ces trois domaines, mais je voulais d'abord faire un rapide survol des infrastructures de

and their role in the financial system. FMIs, such as Canada's wholesale payment system, the large value transfer system, act as a hub for financial transactions.

In turn, banks and other financial institutions are connected to FMIs, much like spokes in a wheel. These systems ultimately facilitate the safe and efficient exchange of funds and other financial products between financial market participants. As a result, protecting FMIs from cyber-threats is of the highest importance. With that background, let me tell you a bit more about our first area of focus, ensuring that the FMIs that are overseen by the bank are taking appropriate steps to mitigate cyber-threats. Financial market infrastructures themselves internally assess their cyber resilience and also have outside experts perform similar assessments.

Measures are then identified and undertaken to enhance their cyber resilience. In addition, the Bank of Canada, as the overseer, reviews these assessments and action plans to ensure appropriate cybersecurity tools and practices are in place to protect the critical systems of FMIs. This is an ongoing process because cyber-threats are constantly evolving.

For our second area of focus, collaborating with others to improve the cyber resilience of the financial system, we use our Financial System Review to draw attention to cyber-threats as we did last November. We also undertake more ad hoc initiatives. Let me give you a few examples.

In partnership with the main participants in the wholesale payments system, the bank is leading a business continuity initiative to support rapid recovery should a key participant in the payment system be affected by a serious cyber event. We've helped draft international guidance on cyber resilience for FMIs, which has been used to help assess the cyber posture of FMIs both within Canada and abroad.

We are contributing to the cyber work being undertaken by a number of international forums including the G-7 Cyber Expert Group and we are also planning a number of table-top exercises with FMIs to better understand how they would respond to and recover from a cyberattack.

Finally, our third area of focus is to ensure the bank itself is resilient to cyber-threats. We are engaged in a continuous process of reviewing our cyber risk management practices against international standards and we are making necessary investments to defend against a rapidly evolving array of cyber-threats.

marchés financiers, ou IMF, et de leur rôle au sein du système financier. Les IMF, par exemple le Système de transfert de paiements de grande valeur (le système de paiements de gros utilisé au Canada), servent de plateforme centrale pour les transactions financières.

Les banques et les autres institutions financières sont, pour leur part, liées aux IMF comme les rayons d'une roue. Ces infrastructures favorisent, en définitive, la sûreté et l'efficacité des échanges de fonds et de produits financiers entre les participants du marché financier. Il est donc de la plus haute importance de protéger les IMF contre les cybermenaces. Dans ce contexte, laissez-moi vous parler un peu plus de notre première priorité, s'assurer que les IMF soumises à la surveillance de la banque prennent les mesures appropriées pour atténuer les cybermenaces. Les infrastructures de marchés financiers évaluent leur propre cyberrésilience à l'interne, et elles demandent aussi à des experts de l'extérieur de procéder à de telles évaluations.

Des mesures sont ensuite déterminées et entreprises pour améliorer la cyberrésilience. De plus, à titre de surveillant, la Banque du Canada étudie ces évaluations et plans d'action, veillant ainsi à ce que des outils et des pratiques de cybersécurité adéquats soient en place pour protéger les systèmes essentiels des IMF. Il s'agit d'un processus continu, puisque les cybermenaces ne cessent d'évoluer.

Pour ce qui concerne notre deuxième priorité — collaborer avec d'autres parties pour accroître la cyberrésilience du système financier —, nous nous servons de la Revue du système financier pour attirer l'attention sur les cybermenaces, comme nous l'avons fait en novembre dernier. Nous entreprenons également d'autres initiatives ponctuelles. En voici quelques exemples :

La banque pilote un projet sur la continuité des opérations en partenariat avec les principaux participants au système de paiement de gros afin de faciliter un rétablissement rapide dans l'éventualité où un participant clé dans le système de paiement serait victime d'un cyberincident grave. Nous avons contribué à la rédaction de lignes directrices internationales sur la cyberrésilience des IMF, qui a aidé à évaluer la posture de cybersécurité de ces infrastructures au Canada et à l'étranger.

Nous participons aux travaux en matière de cybersécurité entrepris par certains forums internationaux, y compris le Groupe d'experts du G7 sur la cybersécurité et nous prévoyons également des simulations en salle avec les IMF afin de mieux comprendre comment elles réagiraient en cas de cyberattaque et reprendraient leurs activités par la suite.

Enfin, notre troisième priorité consiste à veiller à ce que la banque puisse elle-même résister aux cybermenaces. Pour ce faire, nous nous livrons à un processus d'examen continu de nos pratiques de gestion des cyberrisques par rapport aux normes internationales, et nous faisons les investissements nécessaires

[Translation]

Thank you for your attention.

[English]

I would be happy to answer any questions.

Judy Cameron, Senior Director, Legislation, Approvals and Strategic Policy, Office of the Superintendent of Financial Institutions Canada: Thank you for the invitation to appear before the committee today.

As you all know, OSFI is the prudential regulator of federal financial institutions, including Canada's largest banks and insurance companies. I'm Judy Cameron, Senior Director, Legislation, Approvals and Strategic Policy and I am here with my colleague Theresa Hinz.

[Translation]

I want to start by commending the committee for undertaking this study. As my colleagues have noted, technology has had a significant and positive impact on how financial institutions operate, but has also increased their exposure to cyberattacks.

[English]

The committee's study of cybersecurity, including cyber-threats to Canada's financial sector, is timely and important. My colleagues from Finance Canada and the bank have described their initiatives to promote the resilience of Canada's financial sector to cyberattacks. I'd like to complement their remarks by touching on three themes. The first is reporting of major cyber incidents; the second is the unique nature of cyber risks and what it means for OSFI's approach; and the third is OSFI's guidance on outsourcing to third parties.

Let me start with reporting.

[Translation]

I understand why members of the committee are interested in centralized reporting of cyber-threats. This type of reporting could yield valuable information across diverse sectors of the economy.

[English]

OSFI expects the largest financial institutions to notify us when they observe a major cyber incident. These incidents should be reported even if they did not result in an observable cyber event, such as an online outage. We focus on major cyber

pour nous défendre contre toute une gamme de cybermenaces en rapide évolution.

[Français]

Merci de votre attention.

[Traduction]

Je me ferai maintenant un plaisir de répondre à vos questions.

Judy Cameron, directrice principale, Législation, approbations et politique stratégique, Bureau du surintendant des institutions financières Canada : Merci de m'avoir invitée à prendre la parole devant le comité aujourd'hui.

Comme vous le savez tous, le BSIF est l'instance de réglementation prudentielle des institutions financières fédérales, y compris des plus grandes banques et sociétés d'assurances du Canada. Je m'appelle Judy Cameron et je suis la directrice principale de Législation, approbations et politique stratégique. Je suis ici avec ma collègue, Theresa Hinz.

[Français]

Je tiens d'abord à féliciter le comité d'avoir entrepris cette étude. Comme l'ont fait remarquer mes collègues, la technologie a eu une incidence importante et positive sur le mode de fonctionnement des institutions financières, mais elle les a également exposées à un risque accru de cyberattaques.

[Traduction]

L'étude de la cybersécurité, aussi bien que des cybermenaces auxquelles le secteur financier canadien fait face, arrive à point nommé et est importante. Mes collègues de Finances Canada et de la Banque du Canada ont traité de leurs initiatives visant à promouvoir la résilience du secteur financier canadien face aux cyberattaques. J'aimerais vous offrir des observations complémentaires en touchant à trois thèmes : les déclarations de cyberincidents d'envergure, la nature singulière des cyberrisques et les implications pour l'approche du BSIF, et les directives du BSIF sur l'impartition.

Parlons d'abord des déclarations de cyberincidents.

[Français]

Je comprends pourquoi les membres du comité s'intéressent à la déclaration centralisée des cybermenaces. Cette façon de faire est susceptible de produire des renseignements précieux englobant divers secteurs d'activité économique.

[Traduction]

Le BSIF s'attend à ce que les plus grandes institutions financières l'informent des cyberincidents importants dont elles ont eu connaissance, même s'ils n'ont pas provoqué de perturbation observable telle qu'une panne des services en ligne.

incidents because they have the potential to disrupt the financial sector. We look for trends in the information we receive and then share important findings with the financial institutions.

Reporting is just one part of the answer. OSFI's main concern is that financial institutions are resilient in the wake of a cyber attack.

Cyber risk is very different from the risks OSFI routinely manages, such as credit and market risk. These classic financial risks are much easier to predict and measure using financial data and indicators. We can use the information to develop standards and rules for managing risks and to make sure financial institutions are complying with our rules.

Cyber risk, on the other hand, is constantly evolving and hard to measure. As a result, OSFI takes a different approach. We don't consider a financial institution's capacity to detect and prevent threats; we put a lot of focus on its cyber resilience. Cyber resilience refers to an institution's ability to anticipate, withstand, contain and rapidly recover from a cyber attack before it compromises operations or harms its customers.

OSFI issued a cybersecurity assessment template to help financial institutions evaluate their readiness to respond to cyber-threats. The template sets out various desirable features of a cybersecurity framework. To complete the self-assessment, an institution needs to reflect on the current state of its cybersecurity practices. Knowing its own state of readiness is the first step in deciding whether it should enhance its cyber defences and recovery strategies.

OSFI also recently conducted a cyber review where we asked some of our larger institutions to respond to a severe but plausible cyber scenario. The scenario involved a data breach of customer information at a third party that led to a spike in bank accounts being hacked and drained of funds.

This review allowed OSFI to assess the institution's detection and prevention capabilities as well as how they might react to a quickly evolving cyber event.

I will turn to cyber risk and outsourcing. Consumers have come to expect continual innovations in banking services. We're aware of this. Over the past 30 years, we have seen the shift from

Nous nous concentrons sur les cyberincidents importants, car ils risquent de perturber le secteur financier. Nous sommes à l'affût des tendances que révéleraient les renseignements que nous recevons, et nous communiquons ensuite ses constatations importantes aux institutions financières.

La déclaration n'est qu'un élément de la réponse. Le BSIF souhaite avant tout que les institutions financières soient résilientes en cas de cyberattaque.

Le cyber risque diffère considérablement des autres facteurs de risque que gère couramment le BSIF, tels que le risque du crédit et le risque du marché. Ces risques financiers classiques sont plus faciles à mesurer et à prévoir au moyen de données et d'indicateurs financiers. Nous pouvons utiliser les renseignements afin d'établir des normes et des règles pour gérer les risques et pour veiller à ce que les institutions financières s'y conforment.

En revanche, le cyber risque est en mutation constante et il est difficile à mesurer. Le BSIF doit donc aborder le cyber risque sous un angle différent. En plus d'examiner la capacité d'une institution à détecter et à prévenir les menaces, nous attachons aussi une grande importance à sa cyber résilience. La cyber résilience renvoie à la capacité d'une institution de prévoir une cyberattaque, d'y résister, de l'endiguer et de s'en remettre rapidement, avant qu'elle ne compromette ses activités ou qu'elle cause du tort à ses clients.

Le BSIF a publié un modèle d'évaluation de la cybersécurité pour aider les institutions financières à déterminer dans quelle mesure elles sont prêtes à réagir aux cybermenaces. Ce modèle énumère les diverses caractéristiques qui devraient figurer dans un cadre de cybersécurité. Pour effectuer l'évaluation, l'institution doit réfléchir à l'état actuel de ses pratiques en matière de cybersécurité. Pour l'institution, la connaissance de son propre état de préparation est la première étape à franchir avant de décider s'il convient ou non de renforcer ses mécanismes de cyberdéfense et ses stratégies de reprise des activités.

Par ailleurs, le BSIF a procédé récemment à un examen de la cybersécurité dans le cadre duquel il a demandé à certaines des plus grandes institutions canadiennes de réagir à un scénario de cyberincident grave, mais vraisemblable. Le scénario prévoyait une atteinte aux données des clients dans les locaux d'une tierce partie qui aurait entraîné une recrudescence du nombre de comptes bancaires piratés et mis à sec.

Grâce à cet examen, le BSIF a pu évaluer les capacités de détection et de prévention des institutions participantes et déterminer comment elles pourraient réagir à un cyberincident qui évoluerait rapidement.

Je vais maintenant parler du cyber risque et de l'impartition. Les consommateurs s'attendent désormais à ce que les banques innovent sans cesse au chapitre des services qu'elles offrent.

cash and cheques to e-transfers and tap-to-pay and the ability to access services through mobile devices from almost anywhere in the world.

This has been possible because financial institutions have leveraged technology to develop highly integrated systems with a wide variety of partners. Because of this reliance on partners, OSFI's outsourcing guidelines set stringent expectations for how financial institutions manage third party relationships. We hold institutions accountable for services they outsource, and we expect them to conduct due diligence on third-party service providers.

We are reviewing the guideline to assess whether it remains appropriate in the context of growing cyber-threats and OSFI's focus on cyber resilience. I want to conclude with a few words about the way forward.

You have heard cyber risks are a shared threat and managing these risks requires a shared understanding of the problem and a coordinated response.

[Translation]

That is why the Office of the Superintendent of Financial Institutions Canada regularly engages with many of the witnesses appearing before this committee.

[English]

OSFI also works with standard setters and expert groups in other countries because Canada's financial institutions are connected to partners around the globe. OSFI is an active member of the G7 Cyber Expert Group, and we also participate in information-sharing initiatives with the Financial Stability Board, the G20 and the Senior Supervisors Group.

OSFI's mandate includes being ever vigilant toward new and growing risks such as those that threaten cybersecurity. That is why we look forward to the recommendations flowing from the committee's study. Thank you, Mr. Chair.

The Chair: Ms. Hinz, do you have anything to say?

Nous sommes conscients de cela. Depuis 30 ans, nous avons vu l'argent comptant et les chèques être supplantés par les virements électroniques et les cartes sans contact. Les services bancaires sont maintenant accessibles presque partout dans le monde grâce aux appareils mobiles.

Ces transformations n'ont été possibles que parce que les institutions financières ont misé sur la technologie pour mettre au point des systèmes fortement intégrés, en collaboration avec un large éventail de partenaires. Comme les institutions financières dépendent de leurs partenaires, les lignes directrices du BSIF en matière d'impartition leur prescrivent de gérer avec la plus grande rigueur possible leurs relations avec des tiers parties. Nous obligeons les institutions financières à rendre compte des services qu'elles externalisent et nous nous attendons à ce qu'elles fassent preuve de diligence raisonnable à l'endroit des tiers fournisseurs de services.

Nous examinons les lignes directrices pour déterminer si elles sont encore pertinentes dans le contexte des cybermenaces grandissantes et de l'importance que nous accordons à la cyberrésilience. En conclusion, j'aimerais vous dire quelques mots sur ce que l'avenir nous réserve.

Vous avez entendu dire que les cyberrisques constituent une menace commune et que leur gestion passe par une compréhension commune du problème et une réponse coordonnée.

[Français]

Pour ces raisons, le Bureau du surintendant des institutions financières s'entretient régulièrement avec bon nombre de témoins qui se présentent devant ce comité.

[Traduction]

Qui plus est, le BSIF collabore avec des organismes de normalisation et des groupes d'experts à l'étranger, car les institutions financières canadiennes ont des partenaires partout dans le monde. Le BSIF participe activement aux travaux du Groupe d'experts en cybersécurité du G7, ainsi qu'à des initiatives de mise en commun de l'information avec le Conseil de stabilité financière, le G20 et le Groupe des superviseurs principaux.

Un des volets du mandat du BSIF consiste à être sans cesse attentif aux risques émergents et croissants, notamment ceux qui menacent la cybersécurité. C'est pourquoi nous avons hâte de prendre connaissance des recommandations qui découleront de l'étude que mène votre comité. Je vous remercie, monsieur le président.

Le président : Madame Hinz, souhaitez-vous ajouter quelque chose?

Theresa Hinz, Director, Approvals and Precedents, Office of the Superintendent of Financial Institutions Canada: No further opening comments.

The Chair: Thank you.

Senator Stewart Olsen: I have a couple of questions dealing with the announcement from yesterday and then another proposal I would like all of your comments on.

The announcement yesterday was very scant on details, and so I'm wondering when we can look at this being up and ready. Both of these are fairly involved, and I am wondering how long it may take before they get a viable organization together.

Ms. Ryan: Great question, senator. I cannot provide you with a firm date when the new centre will open. I would describe the resources as supplementing and augmenting efforts already under way in different departments, principally the Canadian Security Establishment and the RCMP as well as Public Safety. The resources are welcome. The effort that is involved going forward will involve meeting objectives in terms of renewing leadership governance collaboration in the entities that are working together already. The services will continue to be provided, but I don't have a firm date to start operations.

Senator Stewart Olsen: I will ask for everyone to comment. It says to bring together what's already happening and the cyber experts. I did not see anything in here. Is there any provision or should there be a provision for education to get our own homegrown experts, such as working with universities and colleges? It really is a young person's area, and it's rapidly evolving. I'm wondering what you would think. Would you be supportive of an initiative like that?

Ms. Ryan: The budget targets those objectives. It's part of the framing around building a secure and adaptive ecosystem. It speaks to issues like training and bringing along the next wave of people who will have the right training, will bring innovation to the space and build that wider set of skills and abilities to train more people in cyber-resilient security.

Senator Stewart Olsen: Once again, scant on details so I don't know how they will do that, but that's good to hear.

Mr. Morrow: The type of initiative you've spoken of is something we do see happening in other jurisdictions. Other countries are taking the lead in trying to improve education and create a new wave of people to help with this threat. I'm sure the measures in the budget will stand us in good stead in that regard.

Theresa Hinz, directrice, Approbations et précédents, Bureau du surintendant des institutions financières Canada : Non, je n'ai rien à ajouter à la déclaration liminaire.

Le président : Merci.

La sénatrice Stewart Olsen : J'ai deux questions portant sur l'annonce faite hier et j'aimerais aussi obtenir vos commentaires sur une autre proposition.

L'annonce d'hier était très avare de détails. Je me demande donc à quel moment on peut s'attendre à ce que tous les éléments soient mis en place. Les deux entités sont fort occupées, et je me demande combien de temps il faudra avant qu'elles puissent mettre sur pied une organisation viable.

Mme Ryan : C'est une excellente question, madame la sénatrice. Je ne sais pas à quel moment précisément le nouveau centre pourra entreprendre ses activités. Selon moi, les ressources débloquées serviront à appuyer les efforts en cours au sein de divers organismes et ministères, en particulier au Centre de la sécurité des télécommunications, à la GRC et à Sécurité publique Canada. Les ressources sont bienvenues. Ces efforts permettront de renforcer le leadership, la gouvernance et la collaboration au sein des entités qui travaillent déjà ensemble. Les services continueront d'être offerts, mais je ne connais pas la date précise du début des opérations.

La sénatrice Stewart Olsen : Je demanderais à tous les témoins de me faire part de leurs commentaires. On dit que l'objectif est de réunir sous un même toit les activités déjà en cours et les cyberexperts. Je ne vois rien de précis là-dedans. Existe-t-il une disposition — ou devrait-il y en avoir une — prévoyant notamment que les experts canadiens collaborent avec les universités et les collèges? Il s'agit vraiment d'un secteur axé sur les jeunes, qui évolue rapidement. Je me demande ce que vous en pensez. Êtes-vous en faveur d'une initiative de ce genre?

Mme Ryan : Le budget vise à atteindre ces objectifs. Tout cela fait partie de la volonté de bâtir un écosystème sûr et adapté. Il s'agit de questions comme la formation et le recrutement de la prochaine vague de gens qui seront dûment formés et qui feront preuve d'un esprit d'innovation. Il s'agit également de mettre en place un large éventail de compétences et d'aptitudes, en vue de former plus d'employés en sécurité et en résilience des cybersystèmes.

La sénatrice Stewart Olsen : De nouveau, faute de détails, je me demande comment les responsables vont s'y prendre, mais c'est une bonne nouvelle.

M. Morrow : D'autres pays mettent déjà en œuvre des initiatives comme celle dont vous avez parlé. Ils assument un rôle de chef de file en tentant d'améliorer les programmes d'éducation et d'attirer une nouvelle vague de gens prêts à lutter contre cette menace. Je suis persuadé que les mesures prévues dans le budget nous seront très utiles à cet égard.

Market forces should also help here as the demand for cyber experts is quite strong. As a result, it will be lucrative for students to invest in that type of education.

Ms. Cameron: I would echo Ron's comments that demand for people with these skills is very strong, and we know, through dialogue with our institutions and other regulators, because demand is strong it's sometimes hard to track and keep these skills, and that's very important to all of us to help deal with cyber-threats. I would echo the comments of my colleagues that a program to support education is valuable, but how it all plays out, we have little information.

Senator Tannas: Thank you for being here. I wanted to try and understand where Canada is relative to other G7 countries.

Ms. Ryan, around the national cybersecurity strategy and Canadian Institute for Cybersecurity, are there other countries that have a similar strategy document and a centre for security up and running or are we at the forefront of this?

Ms. Ryan: From our work at the G7 table, I'm confident to say all countries are moving ahead very quickly to put in place similar arrangements and information sharing. In terms of a country that is a good model for Canada, I think the U.K. has done very good work with their cyber centre.

They typically publish a number of documents. Their annual report from last year was a good source in terms of the type of threats and how they've organized themselves as a centre to respond. So it's a similar type of model.

Senator Tannas: How long have they been around for?

Ms. Ryan: I would have to get back you on that, senator.

Senator Tannas: On a similar theme for Canada's financial institutions and for the Bank of Canada, could you give us a sense of where the Bank of Canada is compared to other similar organizations and functions in different countries? Where are Canadian financial institutions compared to the other G7 countries?

Mr. Morrow: For the Bank of Canada, I'll address the question along two dimensions. First is the work we're doing to help ensure the financial market infrastructures we oversee have a good, resilient set of cyber plans. I would say we are amongst the leaders in our global peers in working with the FMIs to

Les forces du marché devraient aussi nous aider, en ce sens que la demande de cyberexperts est assez forte. Il sera donc rentable pour les étudiants d'investir dans ce type d'éducation.

Mme Cameron : Comme vient de le dire Ron, la demande de personnes possédant ces compétences est très forte. D'après nos discussions avec les institutions et les autres organes de réglementation, nous savons que, comme la demande est forte, il est parfois difficile de recruter et de garder des gens ayant ces compétences. Pour nous tous, il est très important de compter sur un tel effectif pour lutter contre les cybermenaces. À l'instar de mes collègues, je pense qu'un programme d'appui à l'éducation est utile. Toutefois, nous avons peu de renseignements sur la suite des choses.

Le sénateur Tannas : Je vous remercie d'être ici aujourd'hui. J'aimerais comprendre la situation du Canada par rapport aux autres pays du G7.

Madame Ryan, on a parlé de la Stratégie nationale de cybersécurité du Canada et du Centre canadien pour la cybersécurité. Est-ce que d'autres pays disposent déjà d'une stratégie et d'un centre semblables, ou sommes-nous à l'avant-garde à cet égard?

Mme Ryan : Je suis convaincue que tous les pays du G7 agissent très rapidement pour mettre en place des arrangements et des mécanismes d'échange de renseignements semblables aux nôtres. Je pense que le Royaume-Uni peut être un bon modèle pour le Canada, car ce pays a fait de l'excellent travail avec son centre de cybersécurité.

Le Royaume-Uni publie habituellement un certain nombre de documents. Le rapport annuel de l'an dernier était une bonne source d'information sur les types de menaces et la façon dont le centre s'est organisé pour réagir à celles-ci. Il s'agit donc d'un modèle semblable.

Le sénateur Tannas : Depuis combien de temps ce centre existe-t-il?

Mme Ryan : Il faudrait que je fasse des recherches à ce sujet, monsieur le sénateur.

Le sénateur Tannas : Pour ce qui est des institutions financières canadiennes, pourriez-vous nous donner une idée de la situation de la Banque du Canada par rapport à des organisations semblables dans d'autres pays? Comment les institutions financières du Canada se comparent-elles à celles des autres pays du G7?

M. Morrow : Pour ce qui est de la Banque du Canada, je vais répondre à la question en deux volets. Tout d'abord, nous nous employons à faire en sorte que les infrastructures des marchés financiers que nous surveillons disposent de plans efficaces et résilients en matière de cybersécurité. Je dirais que nous figurons parmi les chefs de file mondiaux en ce qui a trait à la

ensure they have strong plans in place and are as resilient as they can possibly be.

On the second part, in terms of the Bank of Canada's own cyber resiliency, I would say we are in a good position but it is very much a moving target. The bad guys are getting better every day. Like many institutions, there are a large number of attempts every day to try to compromise the systems of the bank and we've been successful thus far. It requires continual investment in technology and human resources to make sure we can stay ahead of the game.

Ms. Cameron: OSFI belongs to a number of international groups. We are part of the Senior Supervisors Group, which are regulatory agencies around the world that discuss a host of common challenges, including cyber. From those discussions, it's my sense every country has a different strategy because the mandates of the regulators are slightly different. By and large, they are taking similar approaches. With the U.K., I would share in the observation that it seems to be a bit ahead and other countries can learn from it — the Netherlands also — but we are not laggards. We are learning from our international colleagues and I'm sure they're picking up some stuff from the Canadian system.

Senator Tannas: That is good to know.

Senator Marwah: I was pleased to read about the Canadian Centre for Cybersecurity. This is a single point of expertise long overdue and it is very welcome.

All of you talked about financial sector vulnerability, and given your backgrounds and institutions, obviously that's what you would talk about. But I believe Ms. Cameron said you are only as good as a shared threat. So in a shared threat, you are only as good as the weakest link. While we talk about the FIs and the insurance companies, what about the other sectors, the telcos, the hydros, the utilities? How do they get drawn into this analysis of cyber-threats? Clearly OSFI has no purview of the telcos; neither does the Bank of Canada. So who draws the other players into this analysis of cyber-threats to say we have to look at this collectivity because as hydro or telcos go down, we are hugely vulnerable. Who brings them together?

collaboration avec les infrastructures des marchés financiers. Cette collaboration nous permet de veiller à ce qu'elles disposent de plans solides et à ce qu'elles soient aussi résilientes que possible.

Deuxièmement, pour ce qui est de la cyberrésilience de la Banque du Canada, je dirais que nous sommes dans une bonne position, mais la situation évolue sans cesse. Les personnes mal intentionnées ne cessent de se perfectionner. Comme dans le cas de bien d'autres institutions, la Banque du Canada doit faire face tous les jours à de nombreuses tentatives visant à porter atteinte à ses systèmes. Jusqu'ici, nous avons toujours réussi à écarter ces menaces. Nous devons continuellement investir dans la technologie et les ressources humaines pour conserver une longueur d'avance.

Mme Cameron : Le BSIF est membre d'un certain nombre de groupes internationaux. Il fait partie du Groupe des superviseurs principaux, soit un regroupement d'organismes de réglementation du monde entier qui discutent de défis communs, dont la cybersécurité. Ces discussions nous ont appris que chacun des pays dispose d'une stratégie différente, car les mandats des organismes de réglementation sont légèrement différents les uns des autres. En gros, ils ont adopté des approches semblables. Je suis d'avis que le Royaume-Uni semble avoir une longueur d'avance et que les autres pays peuvent donc apprendre de son expérience. Je dirais que les Pays-Bas se trouvent aussi dans la même catégorie que le Royaume-Uni. Toutefois, nous ne tirons pas de la patte. Nous apprenons de nos partenaires mondiaux, et je suis persuadée que ceux-ci s'inspirent de certains éléments du système canadien.

Le sénateur Tannas : C'est bon à savoir.

Le sénateur Marwah : J'ai été ravi d'apprendre la création du Centre canadien pour la cybersécurité. C'est une source d'expertise unique attendue depuis longtemps et plus que bienvenue.

Vous avez tous parlé de la vulnérabilité du secteur financier, évidemment, compte tenu de vos expériences et de vos institutions. Or, je crois que Mme Cameron a dit que l'efficacité est tributaire d'une menace commune. Face à une menace commune, notre efficacité est à la mesure du maillon le plus faible. Nous parlons des institutions financières et des compagnies d'assurance, mais qu'en est-il des autres secteurs, des entreprises de télécommunications, d'hydroélectricité, de services publics? Comment sont-elles amenées à effectuer cette analyse des cybermenaces? Il est évident que les entreprises de télécommunications ne sont pas du ressort du BSIF ni de la Banque du Canada. Alors, qui incite les autres acteurs à effectuer cette analyse des cybermenaces? Qui dit : « Nous devons nous pencher là-dessus tous ensemble, car si des entreprises d'hydroélectricité ou de télécommunications sont attaquées, nous serons tous très vulnérables »? Qui amène les autres parties à travailler ensemble?

Ms. Cameron: It is an excellent question. It is beyond OSFI's purview and I turn to Ms. Ryan.

Ms. Ryan: First, I would say that in terms of the Government of Canada, Public Safety has the overall lead in terms of mapping the cybersecurity of the country. That leads them to look at how different systems interact together in terms of financial sector, the telcos, the energy sector. They have active work to assess those risks and respond to them.

I would be keen to note that is one of the higher level objectives of the budget announcement of more than half of billion dollars over the coming five years to strengthen the attention paid to those critical systems, to make sure they are robust and resilient and, as Ron says, they continue to respond to the emerging risks in the best way possible.

I would flag that the bank, in particular, has led work on the resiliency side to test a number of scenarios that would involve risks coming from other sectors. We are pursuing these as active discussions with our G7 partners, in terms of the work I mentioned on third party risks. These can either be from another sector or another part of industry. Assessing those risks and planning measures to harden systems against those risks is actively under way.

Mr. Morrow: I had a couple of things. We have done some work with banks, financial institutions and FMIs to take a look at the sectors for which we are highly dependent, in particular energy, telecom and, to some extent, transportation. The outcome is we identified a number of areas where we had some concerns when it came to energy distribution, electricity, in particular in parts of Ontario, and some concerns around telecom resilience and the concentration of equipment in some areas.

We were able to have some good conversations with folks in the other sectors and learn a bit about what they're doing to remediate those risks and walked away more comfortable and confident in terms of what they were doing.

The new centre and the new initiatives announced in the budget will be even more helpful to try to bring the sectors together to a common table where we can have more detailed and open discussions.

Senator Marwah: Is this new centre going to be the coordinating point for overseeing all risks or is it too early to tell? I understand you mentioned Public Works is taking the leadership role, and they are and they aren't. It has generally been very fragmented and difficult to pull everything together to understand what the vulnerabilities are. Everybody is saying you are doing that. There is not a firm hand in looking at the risks in

Mme Cameron : C'est une excellente question. Comme ce n'est pas du ressort du BSIF, je vais céder la parole à Mme Ryan.

Mme Ryan : D'abord, je dirais qu'au gouvernement du Canada, c'est le ministère de la Sécurité publique qui a la responsabilité générale de cartographier la cybersécurité au pays. Il examine ainsi comment différents systèmes interagissent les uns avec les autres dans les secteurs des finances, des télécommunications et de l'énergie. Il travaille activement à évaluer les risques et à les gérer.

J'aimerais souligner que c'est l'un des objectifs de haut niveau liés à l'annonce budgétaire de plus d'un demi-milliard de dollars pour les cinq prochaines années qui vise à augmenter l'attention accordée à ces systèmes cruciaux, afin de s'assurer qu'ils sont solides et résilients et, comme l'a dit Ron, qu'ils continuent de répondre aux risques émergents de la meilleure façon possible.

Je signale que la banque, en particulier, mène des travaux sur la résilience pour mettre à l'essai un certain nombre de scénarios dans lesquels les risques proviennent d'autres secteurs. Nous poursuivons également les discussions avec nos partenaires du G7 en ce qui concerne les risques liés à des tiers, qui peuvent provenir d'un autre secteur ou d'une autre partie de l'industrie. Nous nous employons activement à évaluer ces risques et à prévoir des mesures pour préparer les systèmes à faire face à ces risques.

M. Morrow : J'ai une ou deux choses à ajouter. Nous avons travaillé avec les banques, les institutions financières et les infrastructures des marchés financiers afin d'examiner les secteurs dont nous sommes fortement tributaires, en particulier les secteurs de l'énergie, des télécommunications et, dans une certaine mesure, des transports. Résultat : nous avons relevé un certain nombre de domaines pour lesquels nous avons certaines préoccupations au chapitre de la distribution d'énergie, de l'électricité — en particulier dans certaines régions de l'Ontario —, de la résilience des télécommunications et de la concentration de l'équipement dans certains secteurs.

Nous avons pu mener de bonnes discussions avec des gens d'autres secteurs et nous renseigner un peu sur la façon dont ils atténuent ces risques; nous en sommes ressortis plus à l'aise et rassurés quant à ce qu'ils faisaient pour gérer ces risques.

Le nouveau centre et les nouvelles initiatives annoncés dans le budget seront encore plus utiles pour réunir les secteurs à une même table afin de tenir des discussions plus détaillées et plus ouvertes.

Le sénateur Marwah : Ce nouveau centre servira-t-il de point de coordination pour surveiller tous les risques, ou est-il trop tôt pour le dire? Vous avez mentionné, je crois, que le ministère des Travaux publics assumera le leadership, mais en un sens, il le fera et il ne le fera pas. C'est en général très fragmenté; il est très difficile de réunir tous les éléments pour comprendre quelles sont les vulnérabilités. Personne n'agit d'une

totality rather than every sector doing their piece and without understanding what gets dropped in the middle.

Ms. Ryan: That is very much the objective of the new effort. It is to bring a new level of leadership, cohesion, collaboration to these efforts that are under way. And the new centre will focus most specifically on risks related to cyber-threats. There remain wider threats to public safety that cross sectors and that wider sense of operational risk contains the set of cyber risks. We will need to continue to pay attention to those, but the new centre will focus more deliberately and in a more coordinative way on those cyber risks that face critical cyber systems.

[Translation]

Senator Dagenais: My question is for Ms. Ryan. Last September, Equifax was the victim of identity theft when the credit card numbers and personal information of more than 209,000 Americans were stolen. Forty days passed before Equifax informed the public of the theft, which gave the fraudsters ample time to act.

The company disclosed very little information about the theft in Canada also. Do you have any authority over these businesses, which work with all financial institutions and manage such quantities of personal information? Is there a time frame within which the financial institution must inform its clients that they are victims of identity theft?

Ms. Ryan: That is an excellent question, senator. I will give you a more precise answer in English.

[English]

The question you pose does cross a number of responsibilities. In the first instance PIPEDA specifies the requirements businesses must follow in protecting the private information of Canadians in a similar type of institution as you describe.

Further, the reporting of cyber breaches are covered by that act, depending on the type of institution involved and for the credit agencies, as well as different regulators if they be provincial or federal. That fabric of requirements on businesses as well as the oversight, depending on what type of personal information they have, are in place. In terms of financial sector risk, we do think about these risks in terms of "at what point do they pose a systemic risk for the financial sector?" That's a separate margin of work that plays in your space.

main ferme pour examiner l'ensemble des risques; chaque secteur agit en vase clos, sans comprendre ce qui se passe ailleurs.

Mme Ryan : C'est tout à fait l'objectif des nouvelles initiatives : accroître le leadership, la cohésion et la collaboration dans les efforts qui sont actuellement déployés. Le nouveau centre mettra l'accent plus particulièrement sur les risques liés aux cybermenaces. Il y a encore des menaces étendues à la sécurité publique qui touchent tous les secteurs, et ces risques opérationnels au sens plus large englobent l'ensemble des cyberrisques. Nous devons continuer d'y porter attention, mais le nouveau centre se penchera d'une façon plus délibérée et plus coordonnée sur les cyberrisques auxquels font face les cybersystèmes essentiels.

[Français]

Le sénateur Dagenais : Ma question s'adresse à Mme Ryan. En septembre dernier, Equifax a été victime d'un vol d'identité, alors que les numéros de carte de crédit et les renseignements personnels de plus de 209 000 Américains ont été volés. Equifax a mis 40 jours avant de rendre ce vol public, ce qui a laissé amplement de temps aux fraudeurs pour agir.

Au Canada également, l'entreprise a fourni très peu d'information concernant le vol. Avez-vous une certaine autorité sur ces entreprises qui sont reliées à toutes les institutions financières et qui gèrent une telle quantité de données personnelles? De quel délai dispose l'institution financière pour informer ses clients lorsqu'ils ont été victimes d'un vol d'identité?

Mme Ryan : C'est une excellente question, sénateur. Afin de vous fournir une réponse plus précise, je vais m'exprimer en anglais.

[Traduction]

La question que vous posez concerne un certain nombre de responsabilités. D'abord, la Loi sur la protection des renseignements personnels et les documents électroniques précise les exigences que les entreprises doivent respecter relativement à la protection des renseignements personnels des Canadiens, notamment pour le type d'institution comparable à celle dont vous parlez.

Ensuite, le signalement des atteintes aux données est visé par cette loi, selon le type d'institution, et pour les agences d'évaluation de crédit, ainsi que différents organismes de réglementation, qu'ils soient provinciaux ou fédéraux. Cet ensemble d'exigences à l'égard des entreprises, ainsi que la surveillance, selon le type de renseignements personnels qu'elles conservent, sont en place. Sur le plan des risques liés au secteur financier, nous cherchons à déterminer à quel moment ils constituent un risque systémique pour le secteur financier. C'est une marge distincte de travail qui est en cause.

[Translation]

Senator Dagenais: On the same topic, with the information collected, have you analyzed the cyber attacks on our financial institutions? Perhaps Mr. Morrow can tell me. I don't think you will have the answer, but could you tell us where in the world the perpetrators of these attacks are located?

[English]

Ms. Ryan: I am happy to let my colleagues answer as well. I see the real expertise for that type of analysis as being the CSE, the Canadian Security Establishment. It is a balance they have to strike in terms of doing their surveillance and analysis of risks that play out in cyberspace and working with specific institutions, businesses, and so on, to improve their resiliency and to work together in a collaborative and trusted space versus having a fulsome reporting of all attacks and incidents to the public.

I would assure you that type of analysis is in real time. It's more than daily. It's their constant vigilance. In terms of public reports, I would refer to institutions like CSE or Public Safety who are close to that surveillance.

[Translation]

Senator Dagenais: Perhaps centralizing the information might result in a tightening of the rules.

Would some cyber attacks be kept secret because the banks prefer to take the loss and compensate the victims in order to prevent creating a climate of concern among their clients?

[English]

Ms. Cameron: We have told our institutions we expect them to report any kind of material cyber incident. We don't expect the banks to keep secrets from us but we don't know what we don't know.

[Translation]

Senator Dagenais: I tried. Thank you.

[English]

Ms. Cameron: We don't oversee what happens in a bank. We can't really comment on what we don't hear about.

Senator Wetston: Thank you for coming here today.

[Français]

Le sénateur Dagenais : Je reste sur le même sujet. À partir des signalements que vous avez colligés, avez-vous fait une analyse des cyberattaques qui se sont produites dans les institutions financières? Peut-être que M. Morrow pourra me le dire. Je ne crois pas que vous ayez la réponse, mais pourriez-vous nous dire où se trouvent, dans le monde, les auteurs de ces attaques?

[Traduction]

Mme Ryan : Je serai heureuse de laisser mes collègues répondre également. La véritable expertise pour ce type d'analyse se trouve au Centre de la sécurité des télécommunications, ou CST, qui doit établir un juste équilibre entre, d'une part, la surveillance et l'analyse des risques dans le cyberspace ainsi que le travail avec les institutions et les entreprises, notamment, afin d'améliorer leur résilience et de collaborer dans un espace de confiance et, d'autre part, le signalement exhaustif au public de toutes les attaques et de tous les incidents.

Je vous assure que ce type d'analyse se produit en temps réel, plus que quotidiennement. La vigilance est constante. En ce qui concerne les signalements publics, je m'adresserais à des organismes comme le CST ou au ministère de la Sécurité publique, qui sont très près de cette surveillance.

[Français]

Le sénateur Dagenais : Le fait de centraliser l'information permettrait peut-être de resserrer les règles.

Est-ce que certaines cyberattaques seraient demeurées secrètes parce que les banques ont préféré accuser une perte et indemniser les victimes pour éviter de créer un climat d'inquiétude chez leur clientèle?

[Traduction]

Mme Cameron : Nous avons dit à nos institutions que nous attendions d'elles qu'elles signalent tout incident cybernétique. Nous ne nous attendons pas à ce que les banques nous cachent des choses, mais nous ne savons pas ce que nous ne savons pas.

[Français]

Le sénateur Dagenais : C'était une tentative. Je vous remercie.

[Traduction]

Mme Cameron : Nous ne surveillons pas ce qui se passe dans les banques. Nous ne pouvons pas vraiment faire de commentaire sur ce dont nous n'entendons pas parler.

Le sénateur Wetston : Je vous remercie de votre présence aujourd'hui.

Let me follow up on the last comment here about what you know and what you don't know, which is always challenging. You are, of course, aware of the fact securities regulators have had some role in this area. As you know, from my background, I've spent some time in that area. I've done a lot of work personally on the principles of financial markets infrastructure, unfortunately, because it is well beyond my space.

On this last issue of disclosure, which I think is really important — and Ms. Cameron, I'm not directing it to you necessarily as you might all have a comment. The CSA has put out guidelines in this area and requires reporting issuers, and the banks are reporting issuers, to report and disclose publicly any cyberattacks or threats, material matters. I'm not sure if you review those as opposed to what is reported to you. How much time do you spend on that?

The SEC just announced updating because most of our banks and financial institutions are interlisted as you also know. The SEC now requires enhanced disclosure. I think Mr. Clayton has gone further in the guidelines that he expects with respect to this area. Disclosure and transparency are important. Do you have comments with respect to the extent of disclosure and the fact of its importance beyond the banks telling you what is going on?

Ms. Cameron: OSFI has a different regime from the security regulators, as I'm sure you know. When we get information, we don't disclose it. We are prevented from disclosing it.

We have this expectation that our major financial institutions report major cyber incidents to us. As with the CSA's regulations, what is material? It's a bit like beauty is in the eye of the beholder.

We do get reporting, but we don't get a large amount of reporting. I do have the details. Banks have reported eight major incidents since 2016. We also get them to advise us of noteworthy cyber incidents. We usually get two or three noteworthy cyber incidents per quarter. From a security commission's perspective, "material" probably means does it have impact on their financial results and hence their share price. You would be the expert in this field.

Senator Wetston: It's getting close, that's for sure.

Permettez-moi de revenir sur votre dernière remarque à propos de ce que vous savez et de ce que vous ne savez pas, ce qui est toujours un défi. Vous savez, bien sûr, que les organismes de réglementation des valeurs mobilières jouent un rôle à cet égard. Comme vous le savez, j'ai déjà travaillé dans ce domaine. Personnellement, j'ai beaucoup travaillé sur les principes de l'infrastructure des marchés financiers, malheureusement, car cela va bien au-delà de mon champ de compétence.

Au sujet des signalements, que je trouve très importants — et je n'adresse pas ma question nécessairement à Mme Cameron, car vous avez peut-être tous une observation à formuler —, les Autorités canadiennes en valeurs mobilières ont publié des lignes directrices dans ce domaine et exigent que les émetteurs assujettis — et les banques sont des émetteurs assujettis — signalent et divulguent publiquement toutes les cyberattaques ou menaces importantes. Je ne sais pas si vous les examinez par rapport à ce qui vous est signalé. Combien de temps y consacrez-vous?

La Commission des valeurs mobilières vient d'annoncer une mise à jour, car comme vous le savez, la plupart de nos banques et de nos institutions financières sont intercotées. La Commission des valeurs mobilières exige maintenant une meilleure divulgation. Je pense que M. Clayton est allé un peu plus loin quant aux lignes directrices auxquelles il s'attend à cet égard. La divulgation et la transparence sont importantes. Avez-vous des observations à formuler au sujet de l'ampleur de la divulgation et de son importance au-delà du simple fait que les banques vous signalent ce qui se passe?

Mme Cameron : Comme vous le savez sûrement, le Bureau du surintendant des institutions financières a un régime différent de celui des organismes de réglementation des valeurs mobilières. Quand nous obtenons des renseignements, nous ne les divulguons pas. Nous ne le pouvons pas.

Nous nous attendons à ce que les principales institutions financières nous signalent les cyberincidents majeurs. Pour ce qui est des règlements des Autorités canadiennes en valeurs mobilières, qu'entend-on par « important »? Comme la beauté, l'importance est une notion subjective.

Nous avons des signalements, mais pas un nombre considérable. J'ai ici les détails. Les banques ont signalé huit incidents majeurs depuis 2016. Nous leur demandons également de nous informer des cyberincidents notables. Nous recevons habituellement deux ou trois signalements de cyberincidents notables par trimestre. Du point de vue de la Commission des valeurs mobilières, un incident « important » signifie probablement qu'il a des répercussions sur ses résultats financiers et, par conséquent, sur le cours de ses actions. Vous êtes le spécialiste dans ce domaine.

Le sénateur Wetston : C'est presque cela, c'est certain.

Ms. Cameron: These incidents have not compromised their operations in a material way.

Senator Wetston: I see. The only reason I'm pursuing this is both the U.S. and Canada are getting closer on disclosure. With all our interlisted companies, that's helpful. However, on both sides of border companies are expected to provide tailored, entity-specific, non-boilerplate information — you hope — about cybersecurity preparedness, risks and incidents. I'm asking whether or not you are aware of that or think about it in those terms. I recognize the confidentiality aspect with reporting to OSFI, which I have always had some questions about. However, I'm saying this particular area might help fill that void and I think it may be important. Mr. Morrow or Ms. Ryan may have some comment, too. I think it's an important area.

Ms. Cameron: I am aware of the information and I read from the document you are reading from a few days ago. That is the kind of information OSFI expects institutions to provide but in a more detailed fashion than what they would release in a public statement.

Senator Wetston: That's helpful. I think reporting is important.

I have a lot of materials. I have been reading and I can't wait to ask questions. I liked what Senator Marwah is pursuing. A leader of another organization, in talking about the ecosystem, described it this way: "As one leader put it, my risk is your risk and your risk is my risk." I thought that was an interesting way of putting it.

Ms. Cameron: Yes. This is the weakest link comment.

Senator Wetston: Are there standards or protocols generally to address that kind of issue? I see it as a waterfall of risk. I realize in the budget you announced some new initiatives and they are important, but what have you done to date at OSFI, or at finance, or at the bank, to address that particular issue?

Ms. Cameron: Their dependence or the impact of the risks of others on —

Senator Wetston: What are you doing to minimize them?

Senator Marwah was preceding me. Mr. Morrow, I have your paper here. I don't know who gave it to me. Maybe it was something you supplied. It was written recently. Maybe I'll supply it so you have it. It's *Cyber Security: Protecting the Resiliency of Canada's Financial System*. You are one of the

Mme Cameron : Ces incidents n'ont pas nui à leurs opérations d'une façon importante.

Le sénateur Wetston : Je vois. La seule raison pour laquelle je m'intéresse à cette question, c'est que les États-Unis et le Canada se rapprochent sur le plan de la divulgation. Avec toutes nos entreprises intercotées, c'est utile. Cependant, des deux côtés de la frontière, on s'attend à ce que les entreprises fournissent des renseignements personnalisés, propres à l'entité et non standard — on l'espère — à propos de l'état de préparation, des risques et des incidents relatifs à la cybersécurité. Je demande si vous êtes au courant de cela ou si vous le voyez de cette façon. Je comprends l'aspect confidentiel lié aux signalements au BSIF, et j'ai toujours eu des questions à ce sujet. Je dis toutefois que cet aspect pourrait contribuer à combler ce vide, et je crois que ce serait important. M. Morrow ou Mme Ryan ont peut-être aussi des commentaires à faire là-dessus. Je pense que c'est un aspect important.

Mme Cameron : J'en suis consciente et j'ai lu le document que vous citez il y a quelques jours. C'est le genre de renseignements que le BSIF s'attend à ce que les institutions lui fournissent, mais d'une façon beaucoup plus détaillée que dans une déclaration publique.

Le sénateur Wetston : C'est utile. Je pense que les signalements sont importants.

J'ai beaucoup de documents. J'ai fait beaucoup de lecture, et il me tarde de poser mes questions. J'ai bien aimé le point qu'a soulevé le sénateur Marwah. Le dirigeant d'une autre organisation, à propos de l'écosystème, a dit : « Comme l'a indiqué un dirigeant, mon risque est le vôtre, et votre risque est le mien. » J'ai trouvé que c'était une manière intéressante de voir les choses.

Mme Cameron : Oui. Cela rejoint le commentaire sur le maillon le plus faible.

Le sénateur Wetston : Existe-t-il des normes ou des protocoles, en général, pour régler ce genre de problème? Je le vois comme une cascade de risques. Dans le budget, on a annoncé de nouvelles initiatives importantes, mais qu'avez-vous fait jusqu'ici au BSIF, au ministère des Finances ou dans les banques pour régler ce problème?

Mme Cameron : Leur interdépendance ou les répercussions des risques sur les autres...

Le sénateur Wetston : Que faites-vous pour réduire au minimum les risques?

Le sénateur Marwah a soulevé cette question avant moi. Monsieur Morrow, j'ai ici votre document. Je ne sais pas qui me l'a remis. Peut-être l'avez-vous fourni au comité. C'est un document qui a été rédigé récemment. Je peux vous le fournir. Il est intitulé *Cyber Security: Protecting the Resiliency of*

authors. You emphasize cooperation and coordination, not just within government, within the public and private sector which is why I'm pursuing this. That's important particularly if you go beyond financial services and not all financial services are federal. Any comments?

Mr. Morrow: Two dimensions; first, in terms of a framework to ensure people are achieving the right level of cyber resiliency, they are over the bar and you are correctly measuring the bar. There are a number of frameworks in the world to measure cybersecurity preparedness. Most of these frameworks are flexible; any one is the same as the others. We have adopted a particular framework and hold the FMIs up to a certain level of maturity within that framework and are able to demonstrate it.

In addition, to test interconnectedness, that's where tabletop exercises come into play. Having exercises where you have not just the FMIs, but their participants and a range of others around the table and you test how well people are prepared in a coordinated act in an exercise as a way of helping to guard that resilience.

One final point: I would also note that a host of private and public sector groups have sprung up where people share very detailed, very confidential information about cyber breaches on the view that it's not about competition. Everyone is better off if we share information.

It is happening. Sometimes the challenge is the amount of sharing you can do only goes as wide as the circle of trust you are willing to draw. That's an ongoing challenge.

Senator Wetston: My next question is two parts and deals with the issue of interconnectedness. It was a trigger in the financial crisis, as we all know, and it can be a trigger again in cybersecurity risk or resilience, and interconnectedness can lead to systemic risk. What is your view about that with respect to the cybersecurity threats, particularly in the context of your interconnectedness that exists within financial markets?

Mr. Morrow: It's one of the reasons why cybersecurity is a key vulnerability that we face. A problem at one institution can very quickly spread to another, not necessarily the cyber-threat transmitting itself, but one institution or a central infrastructure is off-line means payments are not flowing, transactions are not flowing, it can create a cascade of failures to other institutions. It is a critical characteristic of this cybersecurity vulnerability we face. It is so very important to ensure everyone is well prepared and everyone is striving to be above a certain bar so there is no obvious weak link to the system.

Canada's Financial System. Vous en êtes l'un des auteurs. Vous mettez l'accent sur la coopération et la coordination, mais pas seulement au sein du gouvernement, dans le secteur public et le secteur privé; voilà pourquoi je soulève cette question. C'est important, en particulier si l'on va au-delà des services financiers, et les services financiers ne relèvent pas tous du fédéral. Avez-vous des commentaires à ce sujet?

M. Morrow : Il y a deux dimensions; d'abord, en fait de cadre permettant de s'assurer que les gens atteignent le niveau approprié de cyberrésilience, qu'ils dépassent les attentes et que l'on évalue correctement les normes, il en existe un certain nombre dans le monde pour mesurer l'état de préparation en matière de cybersécurité. La plupart de ces cadres sont fongibles et sont comparables les uns aux autres. Nous avons adopté l'un de ces cadres; nous maintenons les infrastructures des marchés financiers à un certain niveau de maturité à l'intérieur de ce cadre et nous sommes en mesure de le démontrer.

De plus, des exercices de simulation sont utilisés pour mettre à l'essai l'interconnexion. Lors d'exercices où l'on trouve non seulement les infrastructures des marchés financiers, mais aussi leurs participants et diverses autres personnes, on vérifie dans quelle mesure les gens sont préparés à une action coordonnée, afin de contribuer à préserver cette résilience.

Comme dernier point, je souligne qu'une multitude de groupes des secteurs privé et public ont vu le jour dans le but de permettre aux gens de partager des renseignements très détaillés et très confidentiels au sujet des atteintes à la cybersécurité en partant du principe que ce n'est pas une question de concurrence. Tout le monde est gagnant si nous échangeons des renseignements.

Cela se produit. Le problème, parfois, c'est que la quantité de renseignements que l'on peut communiquer se limite au cercle de confiance que l'on veut tracer. C'est un défi constant.

Le sénateur Wetston : Ma prochaine question comporte deux parties et porte sur l'interconnexion. Elle a été un déclencheur de la crise financière, comme nous le savons tous, et elle peut l'être encore sur le plan du risque ou de la résilience en matière de cybersécurité; l'interconnexion peut mener à un risque systémique. Quelle est votre opinion à ce sujet par rapport aux menaces à la cybersécurité, en particulier dans le contexte de l'interconnexion qui existe au sein des marchés financiers?

M. Morrow : C'est l'une des raisons pour lesquelles la cybersécurité est un facteur de vulnérabilité majeur pour nous. Un problème dans une institution peut très rapidement se propager à une autre; la cybermenace ne se transmettra pas nécessairement, mais le simple fait que le système d'une institution ou d'une infrastructure centrale est en panne signifie que les paiements et les transactions ne se font pas, et cela peut entraîner une cascade de défaillances dans les autres institutions. C'est donc une caractéristique grave de cette vulnérabilité sur le plan de la cybersécurité, et c'est pourquoi il est très important de

Ms. Ryan: The new resources that have been dedicated recognize the importance of critical systems. We have been doing work to identify what are the components of systems that have that deepest interconnectedness that we need to worry about the most. We have been working together. There will be new resources coming for those critical cyber systems, and then beyond we're trying to identify what is the next wider set of concentric circles out? That speaks to the work I mentioned earlier about third-party risks we are pursuing domestically, working with G7 partners to identify the next set of things to worry about.

Senator Wetston: Are you including blockchain technology in that?

Mr. Morrow: The next ring is less about block chain technology and far more about the third-party service providers. If everyone is using Amazon web services for cloud computing, then there is a new vulnerability.

The Chair: I have a couple of quick questions to focus a bit on the agency that was announced yesterday.

Do we understand Public Safety will take the lead in that agency or is it undetermined?

Ms. Ryan: I think it's best to wait for the more detailed announcement, senator. It will have a heavy involvement of the Canadian security establishment.

The Chair: Fair enough, the question of the lead, if it has been determined, isn't publicly available.

Ms. Ryan: The budget documents are the extent of public announcements and a number of details remain to be announced.

The Chair: Very well. Would the same answer apply to this question: To whom will the agency report?

Ms. Ryan: The same answer, senator.

The Chair: Thank you very much. Senator Stewart Olsen started with a very important question. This issue obviously, given the time you are dedicating and we are dedicating to this, is on the plate now. In fact we might even be a bit late to the kitchen. Timing becomes very important. In the document that will be released, will we have a discussion about when this agency will be operative or can you comment now?

veiller à ce que tout le monde soit bien préparé et s'efforce d'atteindre un certain niveau de résilience afin qu'il n'y ait pas de maillon faible évident dans le système.

Mme Ryan : Les nouvelles ressources consacrées à la cybersécurité tiennent compte de l'importance des systèmes essentiels. Nous nous sommes employés à identifier les composantes des systèmes dont l'interconnexion est la plus grande et dont nous devons nous préoccuper le plus. Nous travaillons ensemble. De nouvelles ressources seront affectées à ces cybersystèmes essentiels; nous tentons également de déterminer quel sera le prochain ensemble de cercles concentriques. Cela reflète le travail, dont j'ai parlé plus tôt, concernant les risques liés à des tiers que nous accomplissons au pays, en collaboration avec nos partenaires du G7, pour définir la prochaine série de menaces dont il faudra se préoccuper.

Le sénateur Wetston : Incluez-vous la technologie de chaîne de blocs dans cela?

M. Morrow : Il est moins question de la technologie de chaîne de blocs que des tiers fournisseurs de services. Si tout le monde utilise les services web d'Amazon pour l'informatique dématérialisée, alors il y aura une nouvelle vulnérabilité.

Le président : J'ai quelques brèves questions à poser concernant l'organisme dont on a annoncé la création hier.

Doit-on comprendre que le ministère de la Sécurité publique dirigera cet organisme, ou cela n'a-t-il pas encore été déterminé?

Mme Ryan : Je pense qu'il est préférable d'attendre une annonce plus détaillée, monsieur le sénateur. Le Centre de la sécurité des télécommunications y participera dans une très large mesure.

Le président : Très bien. La question de la direction, si elle a été établie, n'est pas encore publique.

Mme Ryan : Les documents budgétaires se résument aux annonces publiques, et un certain nombre de détails devront être annoncés.

Le président : Très bien. La même réponse s'applique-t-elle à la question suivante : de qui relèvera l'organisme?

Mme Ryan : C'est la même réponse, monsieur le sénateur.

Le président : Merci beaucoup. La sénatrice Stewart Olsen a posé tout à l'heure une question très importante. De toute évidence, considérant le temps que vous y consacrez et que nous y consacrons, cet enjeu est actuellement à l'ordre du jour. En fait, nous sommes peut-être même un peu en retard. Le facteur temps devient très important. Dans le document qui sera rendu public, nous dira-t-on quand cet organisme sera opérationnel? Pouvez-vous nous en parler maintenant?

Ms. Ryan: Senator, I prefer to echo the comments in the first answer, which is that many of these efforts are already under way within the resources that we have. As plans take shape, take place, get the appropriate approvals and so on, we are seized with the urgency of the need and keen to get them up and running.

The Chair: Key language, seized with the urgency of the need, I like that a great deal. I want to amplify what Senator Marwah said and his exploration of the concerns we have around the private sector. Basically, in our economy, I don't think I would be worrying as much about the Canadian banks and their ability to deal with these challenges as I might around pipeline companies or air traffic controllers or "fill in the blanks". So it becomes key in a strategy that we have those linkages as Senator Marwah clearly indicated.

Do you believe there is an understanding at the centre of government that is essential?

Ms. Ryan: Yes, very much so, senator. The budget documents do speak to that need to think of critical systems Canadians rely on, so financial services, transportation, energy, those are of a particular level of attention.

I would draw your attention to the announcement that spoke to the need to also protect Canadian businesses and Canadian citizens in their online existence more generally. That's backed up not just with a trusted source of advice and building the ecosystem, but a very robust and tangible attention to the need to see these attacks as crimes and follow up with investigations and prosecutions so Canadians are protected, Canadian businesses are protected. When we identify certain systems as being more systemic risks to Canadians and Canadian businesses, that is where we are putting additional resources, liaison, governance and leadership going forward.

The Chair: Let me take this opportunity to thank you all for being here today and helping us with our deliberations. You have been extremely helpful because you are very knowledgeable. Thank you also for the work you do on a daily basis serving Canadians. It was a pleasure to have you and we have benefitted from your attendance.

On our second panel, senators, representing Payments Canada, is Justin Ferrabee, Chief Operating Officer, and Martin Kyle, Chief Information Security Officer.

I understand we're going to have an introductory presentation from Mr. Ferrabee and after the senators will undoubtedly have questions for you. Thanks for being here.

Mr. Ferrabee, the floor is yours.

Mme Ryan : Sénateur, je préfère répéter les commentaires faits dans la première réponse, qui sont que beaucoup de ces mesures sont déjà en cours de réalisation, mais que nos ressources sont limitées. À mesure que les plans prennent forme, prennent place, et que les approbations nécessaires sont obtenues et ainsi de suite, nous sommes saisis par l'urgence du besoin et nous sommes portés à accélérer les choses.

Le président : J'aime beaucoup l'expression « saisis par l'urgence du besoin ». Je tiens à souligner ce que le sénateur Marwah a dit et son analyse des préoccupations que nous avons au sujet du secteur privé. En gros, dans notre économie, je ne pense pas que je m'en ferais autant pour les banques canadiennes et leur capacité de surmonter ces difficultés que pour les sociétés de pipelines, les contrôleurs aériens, ou ce que vous voulez. Il devient donc essentiel, dans une stratégie, que nous ayons ces liens, comme le sénateur Marwah l'a clairement indiqué.

Croyez-vous que, au centre du gouvernement, on comprend que c'est essentiel?

Mme Ryan : Oui, merci beaucoup, sénateur. Il est bel et bien question, dans les documents budgétaires, de la nécessité de se pencher sur les systèmes critiques sur lesquels les Canadiens comptent. Ceux des services financiers, des transports, de l'énergie reçoivent donc une attention particulière.

J'attire votre attention sur l'annonce au sujet de la nécessité de protéger aussi les entreprises canadiennes et les citoyens canadiens sur Internet, de manière plus générale, point de vue qui est soutenu par des conseils dignes de confiance et la construction d'un écosystème, mais aussi une attention bien réelle et concentrée à la nécessité de considérer ces attaques comme des crimes donnant lieu à enquêtes et à des poursuites pour que les Canadiens et les entreprises canadiennes soient protégés. Lorsque nous constatons que certains systèmes posent plus de risques pour les Canadiens et les entreprises canadiennes, nous accroissons les ressources et intensifions la liaison, la gouvernance et le leadership.

Le président : Permettez-moi de tous vous remercier d'être ici aujourd'hui pour nous aider dans nos délibérations. Vous êtes extrêmement utiles en raison de vos connaissances. Je vous remercie aussi du travail que vous faites quotidiennement au service des Canadiens. Cela a été un plaisir de vous accueillir et votre présence nous est profitable.

Notre deuxième groupe, sénateurs, représente Paiements Canada et se compose de Justin Ferrabee, chef des opérations, et Martin Kyle, dirigeant principal de la sécurité de l'information.

D'après ce que je comprends, M. Ferrabee va nous présenter un exposé préliminaire, après quoi les sénateurs auront sans aucun doute des questions à lui poser. Merci d'être venu.

Monsieur Ferrabee, vous avez la parole.

Justin Ferrabee, Chief Operating Officer, Payments Canada: Thank you, Mr. Chair and committee members, for inviting Payments Canada to contribute to your study and report on cybersecurity and cyberfraud. I am Justin Ferrabee, joined by my colleague Martin Kyle, Chief Information Security Officer.

I will spend a few moments helping you position Payments Canada, formerly the Canadian Payments Association, in the financial system before delving into Payments Canada's approach to cybersecurity, fraud and some of the outstanding issues and concerns we feel have yet to be addressed.

Payments Canada is Canada's financial market infrastructure for payments. We design and operate Canada's national clearing and settlement systems and facilitate the interaction of those systems with other payment networks and financial market infrastructures. While Payments Canada is a little-known entity to most Canadians, it plays an essential role in the economy and day-to-day operations of financial institutions and businesses across the country.

Payments Canada's systems ensure payments between financial institutions representing the aggregation of payments made by individual Canadians, businesses and governments are safely and securely completed each and every day.

We are guided by our mandate and the public policy objectives of safety, soundness and efficiency of the Canadian clearing and settlement system. These objectives are enshrined in our legislation under the Department of Finance, namely the Canadian Payments Act.

Financial institutions are members and are required to pay Payments Canada and to fund our operations. Our systems are overseen by the Bank of Canada because of their importance to the stability of the overall financial system.

Payments Canada does not operate at the retail layer of the payments value chain where emerging digital payment technologies are conceived. Our focus is at the macro or infrastructure level and is concerned with ensuring financial claims between financial institutions can be settled efficiently and without risk.

However, in consultation with members and stakeholders, we maintain a framework of rules and standards that facilitates the exchange of payments and the development of emerging payment products and services, an area of particular focus as we look to modernize our systems.

Justin Ferrabee, chef des opérations, Paiements Canada : Je vous remercie, monsieur le président et membres du comité, d'avoir invité Paiements Canada à contribuer à votre étude des questions et préoccupations relatives à la cybersécurité et à la cyberfraude pour en faire rapport. Je m'appelle Justin Ferrabee et je suis accompagnée de mon collègue, Martin Kyle, dirigeant principal de la sécurité de l'information.

Je prendrai quelques minutes pour vous aider à placer Paiements Canada — anciennement l'Association canadienne des paiements — dans le contexte du système financier avant d'entrer dans les détails de l'approche de Paiements Canada à l'égard de la cybersécurité et de la cyberfraude et d'aborder certaines questions et préoccupations qui, selon nous, n'ont toujours pas été réglées.

Paiements Canada est l'infrastructure de marchés financiers du Canada relative aux paiements. Nous concevons et mettons en œuvre les systèmes nationaux de compensation et de règlement du Canada, et nous assurons l'interaction de ces systèmes avec d'autres réseaux de paiements et infrastructures de marchés financiers. Paiements Canada est une entité peu connue de la plupart des Canadiens, mais elle joue un rôle essentiel dans l'économie et dans les activités quotidiennes des institutions financières et des entreprises du pays.

Les systèmes de Paiements Canada assurent que les paiements entre les institutions financières, qui représentent l'ensemble des paiements effectués par les particuliers canadiens, les entreprises et les gouvernements, sont effectués en toute sécurité chaque jour.

Nous sommes guidés par notre mandat et les objectifs de politique publique que sont la sûreté, l'efficacité et l'efficience des systèmes de compensation et de règlement canadiens. Ces objectifs sont entérinés dans notre loi en vertu du ministère des Finances : la Loi canadienne sur les paiements.

Les institutions financières qui offrent des services de paiement sont tenues d'être membres de Paiements Canada et de financer nos opérations. Nos systèmes sont sous la surveillance de la Banque du Canada, du fait de notre importance pour la stabilité de l'ensemble du système financier.

Paiements Canada ne fonctionne pas au niveau « détail » de la chaîne des paiements, où sont conçues les nouvelles technologies de paiement numérique. Notre articulation se situe au niveau macro et a pour objet d'assurer le règlement efficace et sans risque des comptes financiers entre les institutions financières.

Cependant, en consultation avec nos membres et nos intervenants, nous tenons à jour un cadre de règles et de normes qui facilite le déploiement de nouveaux produits et services de paiement, un aspect qui nous intéresse tout particulièrement alors que nous cherchons à moderniser nos systèmes et nos règles.

We take our highest priority of safety and soundness seriously. It commands the focus, resources and investments above all other needs, both now and in the future.

This means we design, review, modify and update our systems as we monitor risks. We remain in a constant state of vigilance and respond as required to ensure we manage risk appropriately.

Given the cyber threat environment continues to evolve rapidly, Payments Canada continues to raise its defences against this area of operational risk. We have a cybersecurity action plan based on secure design principles and industry standards. The plan ensures we are constantly watching for and closing gaps to maintain the resiliency of our operations. It means identifying sensitive assets and their environmental context, protecting the infrastructure that contains those assets, detecting threats attempting to compromise the infrastructure, responding to events and incidents and recovering from potential intrusions.

Payments Canada operates within a network of financial institutions, regulators and other financial market infrastructures. Accordingly, we are held to a high standard of security that includes the *Guidance on cyber resiliency for financial market infrastructures*, the SWIFT Customer Security Program and the Cyber Security Framework from the National Institute of Standards.

In turn, we establish rules and standards around the security of payment items and connectivity of systems to which our members must adhere. With our partner banks in the financial sector, we collaborate on cybersecurity and coordinate management across the ecosystem through important industry groups such as the Canadian Financial Services Cybersecurity Governance Council, Cyber Security Specialist Group and Information Sharing and Analysis Centre.

We also plan for high resiliency and participate in interorganizational exercises for business continuity and disaster recovery. We remain connected and share intelligence with partner public agencies and non-governmental organizations in the cybersecurity community. These connections include Public Safety Canada, the Canadian Cyber Incident Response Centre and the Critical Infrastructure Protection Branch, Communications Security Establishment, the Cybersecurity Ecosystem Development, the RCMP National Critical Infrastructure Team and the Canadian Cyber Threat Exchange.

Nous prenons au sérieux notre plus importante priorité de sûreté et d'efficacité. Elle retient l'intérêt, les ressources et les investissements avant tout autre besoin, aujourd'hui et dans un monde modernisé.

Cela signifie que nous concevons, examinons, modifions et actualisons nos systèmes alors que nous surveillons les risques. Nous demeurons constamment vigilants et intervenons au besoin pour nous assurer de gérer les risques de façon appropriée.

Étant donné que les cybermenaces continuent d'évoluer rapidement, Paiements Canada continue d'accroître ses défenses contre ce secteur de risque opérationnel. Nous avons un plan d'action sur la cybersécurité qui est fondé sur certains principes de conception sécurisée et sur les normes de l'industrie. Le plan prévoit de notre part une constante surveillance des lacunes, et leur correction, afin d'assurer la résilience de nos opérations. Il s'agit de reconnaître les biens sensibles et leur contexte environnemental, de protéger l'infrastructure qui les abrite, de détecter les menaces visant à compromettre l'infrastructure, de réagir aux événements et aux incidents et de se rétablir après des intrusions potentielles.

Paiements Canada fonctionne au sein d'un réseau d'institutions financières, d'organismes de réglementation et d'autres infrastructures du marché financier. Par conséquent, nous sommes tenus de respecter des normes de sécurité élevées qui comprennent le *Document d'orientation sur la cyberrésilience pour les infrastructures des marchés financiers*, le Programme de sécurité de la clientèle (PSC) de SWIFT et le Cadre de cybersécurité du National Institute of Standards and Technology.

En retour, nous établissons des règles et des normes auxquelles nos membres doivent adhérer et qui concernent la sécurité des effets de paiement et la connectivité des systèmes. De concert avec nos partenaires du secteur financier, nous collaborons à la cybersécurité et à la coordination de la gestion dans l'ensemble de l'écosystème par l'entremise de groupes importants de l'industrie comme le Conseil canadien de gouvernance en matière de cybersécurité des services financiers, le Groupe de spécialistes de la cybersécurité des institutions financières canadiennes et l'Information Sharing and Analysis Centre.

De plus, nous dressons des plans pour une résilience élevée et participons à des exercices interorganisationnels pour assurer la continuité des activités et la reprise après sinistre. Nous restons également en contact et échangeons des renseignements avec des organismes publics partenaires et des organisations non gouvernementales du milieu de la cybersécurité. Ces liens comprennent Sécurité publique Canada, le Centre canadien de réponse aux incidents cybernétiques et la Direction générale de la protection des infrastructures essentielles, le Centre de la sécurité des télécommunications — Développement des écosystèmes de cybersécurité, l'Équipe nationale des

Working closely with our members, our overseer and our regulator, we are currently undertaking a major program that will result in a modernized infrastructure. We are bringing our focus, discipline and commitment to the safety and soundness principles to this modernization effort and will ensure the modernized environment continues to secure payments for the Canadian economy.

Through this diligence, we are able to see certain gaps that exist outside our control that this body may be able to influence and we would like to discuss those a bit today, if appropriate.

First, there is a clear need for public/private coordination in responding to attacks against critical infrastructure and a single clear point of contact in the public sector for chief information security officers in the private sector. These improvements will help us better share information in a protected fashion and will help us manage and prevent future attacks. We hope the new bodies identified in the 2018 federal government's budget, a Canadian Centre for Cybersecurity and a national cyber crime coordination unit will help to resolve this issue.

Secondly, financial market infrastructures form the backbone of the economy. These systemic cyber systems must be prioritized for recovery with vendors and infrastructure in the event of a widespread disruption. Policy that extends cybersecurity requirements to the supply chain of critical systems will help improve resilience of dependent components to the national infrastructures and the financial system as a whole.

Finally, there is more that could be done to address the cybersecurity skills shortage. There is already a gap in capable people and given the increase and severity of threats, there is a need for policy and strategies to develop, attract and retain skilled workers.

While every organization has a responsibility to protect themselves from cyberattacks, the value of the network, including both public and private entities — doing so as a collective will be much more effective. Moving forward, it will be important to look at cybersecurity as an issue affecting the Canadian economy and our national security as a whole, as there are clear codependencies. Payments Canada is eager to contribute to and support a network defence strategy.

infrastructures essentielles de la GRC et l'Échange canadien de menaces cybernétiques (ECMC).

En étroite collaboration avec nos membres, notre superviseur et notre organisme de réglementation, nous entreprenons actuellement un programme d'envergure qui permettra de moderniser complètement l'infrastructure. Nous mettons l'accent sur les principes de la sécurité et de la solidité dans cette initiative de modernisation et nous nous assurons que l'environnement modernisé continue de garantir les paiements pour l'économie canadienne.

Cette diligence nous permet de déceler certaines lacunes qui échappent à notre contrôle et que votre organisme pourrait influencer. Nous aimerions aborder ces lacunes aujourd'hui.

En premier lieu, il apparaît clairement nécessaire d'assurer une coordination publique-privée pour réagir aux attaques contre les infrastructures essentielles, et aussi de déterminer dans le secteur public un seul point de contact précis pour les dirigeants principaux de la sécurité de l'information du secteur privé. Ces améliorations faciliteront notre partage de l'information — de façon protégée — tout en nous aidant à gérer les attaques futures, et à les prévenir. Nous espérons que les nouveaux organismes énoncés dans le budget de 2018 du gouvernement fédéral — le Centre canadien pour la cybersécurité et l'Unité nationale de coordination de la lutte contre la cybercriminalité — nous aideront à résoudre cet enjeu.

En deuxième lieu, les infrastructures des marchés financiers constituent l'épine dorsale de l'économie. Il faut accorder la priorité à ces cybersystèmes systémiques pour la reprise avec les fournisseurs et l'infrastructure en cas de perturbation généralisée. Une politique qui étend les exigences de cybersécurité à la chaîne d'approvisionnement des systèmes essentiels contribuera à l'amélioration de la résilience des composantes dépendantes aux infrastructures nationales et au système financier dans son ensemble.

En dernier lieu, nous sommes convaincus qu'il serait possible de faire davantage pour remédier à la pénurie de compétences en cybersécurité. Une pénurie de personnes compétentes sévit déjà et, compte tenu de l'augmentation et de la gravité des menaces, il faut élaborer des politiques et des stratégies permettant de former, d'attirer et de retenir des travailleurs qualifiés.

Bien que chaque organisation ait la responsabilité de se protéger elle-même contre les cyberattaques, il sera beaucoup plus efficace d'engager une action collective du réseau à cet effet, englobant les entités publiques et privées. À l'avenir, il sera important de considérer la cybersécurité comme un enjeu qui touche l'ensemble de l'économie canadienne et de notre sécurité nationale, en raison des interdépendances évidentes. Paiements Canada est impatient de contribuer à une stratégie de défense du réseau et de la promouvoir.

Payments Canada's mandate is explicitly focused on safety and soundness. As such, we look forward to the recommendations coming from the committee's study and report. Thank you for your time, and we're happy to take questions.

The Chair: Thank you very much, Mr. Ferrabee. It was a very good presentation.

I'll start questions with the deputy chair.

Senator Stewart Olsen: From what you have outlined, you already have an up-and-running, very good cybersecurity department. How do you see yourself interacting with this new agency? Are you a bit concerned — I know that when you have departments like CSIS or the RCMP, there's not a huge sharing of their security issues. You become very protective of what you see as a threat. I'm not sure how we can overcome that with these new agencies. Could you comment on those two things, please?

Mr. Ferrabee: Yes. First, we don't know enough about what's coming down from the budget to know specifically. We are active across the federal family and in multiple areas. We are assuming those will be a part of it in some way, and we would connect through that or whatever regime is coming forward.

We would be proactive in building those relationships to understand how that works. We'd be first in line, if you will, to participate.

Second, the challenge of sharing information is progressive in that you start with what you can, then you don't share what you can't, and then you build trust, share more, then add conditions and circumstances and safety to share more. As Ron Morrow mentioned, it's the circle trust, and you would like that to get bigger in time. There are conditions and prerequisites for that to happen.

We have experience and have had success in that. We think we can do it. As the awareness of cyber grows, collective interest also grows. We have confidence we will see more of that and some standards for participating.

Martin Kyle, Chief Information Security Officer, Payments Canada: We currently receive threat intelligence information from some of the agencies as they exist now. I expect that will continue in a reorganized fashion in the future. As Justin Ferrabee indicated, as we continue to build the circles

Le mandat de Paiements Canada est explicitement axé sur la sécurité et la solidité du système de paiement. Par conséquent, nous attendons avec impatience les recommandations découlant de l'étude et du rapport du comité. Je vous remercie de votre temps. Nous serons heureux de répondre à vos questions.

Le président : Je vous remercie beaucoup, monsieur Ferrabee. C'était un très bon exposé.

Je vais démarrer la période des questions par la vice-présidente.

La sénatrice Stewart Olsen : D'après votre exposé, vous avez déjà un très bon service de cybersécurité en activité. Comment envisagez-vous votre interaction avec le nouvel organisme? Êtes-vous quelque peu préoccupé? Je sais que les services comme le SCRS ou la GRC ne parlent pas beaucoup de leurs problèmes de sécurité. On devient très protecteur lorsqu'il y a une menace. Je ne suis pas certaine que nous puissions surmonter cet obstacle avec les nouveaux organismes. Pourriez-vous nous dire ce que vous pensez de ces deux choses, s'il vous plaît?

M. Ferrabee : Oui. Premièrement, nous n'avons pas encore suffisamment d'information sur ce qui sera prévu dans le cadre du budget pour connaître les détails. Nos activités touchent l'ensemble de la fonction publique fédérale et divers secteurs. Nous supposons que ces intervenants apporteront leur contribution d'une certaine façon, et que nous allons collaborer dans le cadre de ce processus ou de tout autre régime à venir.

Nous allons bâtir ces relations de façon proactive afin de déterminer comment procéder. Nous sommes en quelque sorte les premiers à vouloir participer.

Deuxièmement, les difficultés concernant l'échange de renseignements évoluent, car on commence par déterminer les renseignements qui peuvent et ne peuvent pas être échangés, puis, à mesure qu'on bâtit la confiance et qu'on met en place des conditions, des procédures et des mesures de sécurité, on peut échanger plus de renseignements. Comme Ron Morrow l'a souligné, il s'agit d'établir un cercle de confiance et de l'élargir au fil du temps. Pour cela, il y a des conditions préalables à respecter.

Nous avons acquis de l'expérience et obtenu du succès en la matière. Nous croyons être en mesure de réussir. L'intérêt collectif grandira à mesure que les intervenants prendront conscience des cybermenaces. Nous sommes persuadés que c'est ce qui se passera de plus en plus et que des normes de participation seront établies.

Martin Kyle, dirigeant principal de la sécurité de l'information, Paiements Canada : Pour le moment, nous recevons des renseignements sur les menaces de la part des organismes actuellement en place. Je m'attends à ce que cet échange de renseignements se poursuive à l'avenir selon un

of trust and increase our maturity, we'll be sharing information back to those agencies.

Senator Stewart Olsen: Good. I look forward to seeing that. Thank you.

Senator Marwah: Thank you both. I really enjoyed reading your briefs and draft remarks.

You make a point here that you feel strongly more could be done to address the cybersecurity skills shortage, and that's certainly people. You go on to say, "It will be important to look at cybersecurity as an issue affecting the Canadian economy and national security as a whole, as there are clear codependencies."

When I read that, I ask, "Who should be assigned this role to pull this together?" Is this a new agency or the many agencies involved already? Who has the responsibility today? Forget about the new one, but who has the responsibility to pull this together to make sure nothing is falling between the cracks?

Mr. Kyle: Public Safety Canada operates a national cross-sector forum on critical infrastructure. That agency brings together parties within 10 identified critical infrastructure areas. It coordinates information, sessions and potentially exercises across those sectors.

Again, as the announcement yesterday suggests, there may be some reorganization. I'm not exactly sure how that will change in the future, but as of today, Public Safety is the agency we interact with at a national level for critical infrastructure.

Senator Marwah: Do you feel what they are doing is adequate, or do you feel in that role alone there are other places that we could do with strengthening our overall strategies and policies?

Mr. Kyle: We're moving down the right path. I was moderating a panel at the OECD a few weeks ago, and a question came up about how critical infrastructure players interact with each other when there's a cyber event. We received some feedback from a U.S. representative that they are conducting cross-sector cyber exercises between, for example, finance, telecom and energy, electrical in particular.

So I know that the critical infrastructure branch has been discussing this possibility with the critical infrastructure players in Canada. We're on that road, but we can continue to do more there.

processus remanié. Comme Justin Ferrabee l'a indiqué, à mesure que nous bâtissons les cercles de confiance et que nous peaufinerons nos méthodes, nous allons continuer d'échanger des renseignements avec ces organismes.

La sénatrice Stewart Olsen : Très bien. J'ai hâte de voir cela. Merci.

Le sénateur Marwah : Merci à vous deux. J'ai bien aimé lire vos mémoires et vos déclarations préliminaires.

Vous dites que vous croyez fermement qu'on peut en faire davantage pour remédier au manque d'effectifs qualifiés en matière de cybersécurité, et cela signifie certainement que nous manquons de personnel. Vous ajoutez ceci : « À l'avenir, il sera important de considérer la cybersécurité comme un enjeu qui touche l'ensemble de l'économie canadienne et de notre sécurité nationale, en raison des interdépendances évidentes. »

En lisant cela, je me demande à qui on pourrait confier une telle tâche. À un nouvel organisme ou aux nombreux organismes déjà en place? Qui est chargé de ce dossier actuellement? Si on fait abstraction du nouvel organisme, qui a la responsabilité de coordonner les efforts afin qu'aucun détail ne soit négligé?

M. Kyle : Sécurité publique Canada organise un forum national intersectoriel sur les infrastructures essentielles qui regroupe des intervenants de 10 secteurs d'infrastructure essentiels désignés. Cela permet de coordonner les activités de renseignement et d'organiser des séances — voire des exercices — dans tous ces secteurs.

Encore une fois, comme l'annonce d'hier l'indique, il pourrait y avoir une certaine réorganisation. Je ne sais pas exactement ce qui sera fait différemment à l'avenir, mais, actuellement, c'est le ministère de la Sécurité publique qui coordonne nos activités à l'échelle nationale en ce qui concerne les infrastructures essentielles.

Le sénateur Marwah : Selon vous, le ministère fait-il le nécessaire, ou croyez-vous que, à ce chapitre, il y aurait d'autres améliorations à apporter à l'ensemble de nos stratégies et politiques?

M. Kyle : Nous sommes sur la bonne voie. Il y a quelques semaines, j'ai servi de modérateur lors d'une discussion organisée par l'OCDE. On s'est demandé notamment comment les intervenants responsables des infrastructures essentielles interagissent en cas de cybermenace. Un représentant des États-Unis a expliqué que, dans son pays, on procède à des exercices de cybermenace qui font appel à divers secteurs comme les finances, les télécommunications, l'énergie et l'électricité.

Je sais donc que la section responsable des infrastructures essentielles a discuté de cette possibilité avec les intervenants responsables des infrastructures essentielles au Canada. Nous

Senator Marwah: In your judgment, which is the best-in-class model you have seen? Is there one you could say has it absolutely right in terms of how they organize themselves, whether it's the U.K. or the EU? The U.S. is more fragmented than us. Which country or model has it right — or as right as you can get?

Mr. Kyle: I can't really comment on other countries' models other than to say every country is facing the same issues that we are right now. The number, the frequency and the severity of cyber attacks are increasing. Just as we are meeting here to study this problem, the nations I have been interacting with are doing the same.

The Chair: Mr. Ferrabee, do you have anything to add? Senator Marwah asked a specific question as to whether there is a model or a country we should be looking at.

Mr. Ferrabee: Specifically around payments infrastructure and the way we interact with other infrastructures, each country varies widely in how it's done. We do work closely with them. We initiated about four years ago a committee of the CEOs of the G7 for addressing these exact issues. I would say we are in the upper quartile in terms of how we're managing. Without disclosing too much on it, we are in the category on a model that seems to work.

The Chair: Thank you very much.

Senator Tannas: Thank you for being here. We talked a lot about what I would call the macro issues of thousands and potentially millions of attempts to breach big systems and so on. But I wonder if maybe you folks are uniquely positioned to talk about some of the micro issues, in addition to what you are trying to do and what concerns everyday Canadians. I'm talking about the hostage-taking of computers where you get to pay somebody \$200 to get your own computer back, and you make a payment to them. There's also the tax department scam things where little old ladies are sending money off, because they think they're behind in their taxes, because somebody contacted them through email or phone. There's also phishing or phony invoices from companies.

I have never heard that anybody suffers redress from that. They send it off, and the response is, "Oh, well, sorry it's gone." Where has it gone? Is there not some way, or is there any discussion about how to coordinate so that money can't just disappear out of a Canadian financial institution to an American financial institution and then wherever it goes — into the ether?

sommes sur la bonne voie, mais nous pouvons encore en faire davantage.

Le sénateur Marwah : À votre avis, quel est le meilleur modèle à suivre parmi ceux que vous avez vus? Y a-t-il un modèle en particulier qui vous semble tout à fait adéquat sur le plan de l'organisation, que ce soit au Royaume-Uni ou au sein de l'Union européenne? L'approche des États-Unis est plus fragmentée que la nôtre. Quel pays ou quel modèle propose la meilleure méthode ou la méthode la plus efficace possible?

M. Kyle : Je ne peux pas vraiment faire de commentaires sur les modèles des autres pays, si ce n'est que tous les pays sont actuellement aux prises avec les mêmes problèmes que nous. Le nombre, la fréquence et la gravité des cyberattaques augmentent. Pendant que nous sommes réunis ici pour étudier ce problème, les pays avec lesquels j'ai interagi font la même chose.

Le président : Monsieur Ferrabee, avez-vous quelque chose à ajouter? Le sénateur Marwah aimerait savoir s'il y a un modèle ou un pays en particulier sur lequel nous devrions nous pencher.

M. Ferrabee : En ce qui concerne plus particulièrement les infrastructures de paiement et la façon d'interagir avec d'autres infrastructures, l'approche varie énormément d'un pays à l'autre. Nous travaillons en étroite collaboration avec les autres pays. Il y a environ quatre ans, un comité de hauts fonctionnaires du G7 a été mis sur pied afin de se pencher précisément sur ces questions. Je dirais que nous nous situons dans le quartile supérieur sur le plan de l'organisation. Sans vouloir en dire trop, je crois que nous sommes dans la catégorie des pays dont le modèle semble fonctionner.

Le président : Merci beaucoup.

Le sénateur Tannas : Merci de votre présence. Nous avons beaucoup parlé de ce que j'appellerais les menaces à grande échelle que constituent notamment les milliers — voire les millions — de tentatives d'atteinte à la sécurité de grands réseaux. Cependant, je me demande si votre position particulière vous permet de vous pencher sur les menaces à petite échelle qui touchent les Canadiens ordinaires en plus de ce que vous essayez de faire. Je parle notamment des rançons qui sont payées à des gens qui prennent des ordinateurs en otage et qui, par exemple, exigent 200 \$ pour débloquent l'accès aux données. Il y a aussi des fraudeurs qui communiquent avec les gens par courriel ou par téléphone pour soutirer de l'argent à de vieilles dames en leur faisant croire qu'elles doivent encore verser de l'impôt à l'agence du revenu. Il y a également de l'hameçonnage ou de fausses factures d'entreprise.

Or, je n'ai jamais entendu parler de l'imposition de mesures réparatoires à cet égard. Les gens envoient l'argent, et on leur dit : « Oh, eh bien, désolé, mais l'argent n'est plus là. » Où est-il allé? N'y a-t-il pas des mesures qui sont prises ou des discussions sur la façon de s'organiser pour que l'argent qui est

In other words, is there any discussion about trying to find ways to get money back for ordinary citizens in all of this discussion?

I know it's one citizen at a time. We've heard there are potentially millions of these things that happen. It has happened to me both in business, for a very large amount of money, and I also had my computer hijacked and I paid the money, and the response is, "Too bad. You lost your money."

Aren't you guys at the forefront of figuring out how to get money back or stop that flow? Is anyone focused on that, or are we just focused on the macro risks to the big banks and hydroelectric and so on? That is important but isn't there an "and" we should be doing here?

Mr. Ferrabee: I will take a first attempt and try not to disappoint you. As a financial market infrastructure, we're down much deeper than that, so we would do the exchange between financial institutions, which is a very small group. They have the customer-facing interface, so they would work with consumers and we would see the FCAC as the agency that would advocate for Canadians on financial matter in terms of financial consumers.

We aren't active at that layer in the payment system. We may have some views or not, but Payments Canada is an infrastructure and our focus is narrow. It's small and important but it doesn't cover consumer activity.

Senator Tannas: If I'm sending a payment somewhere, that is not facilitated by your infrastructure in any way.

Mr. Ferrabee: It would go through our members — the banks — and eventually, at the infrastructure layer, when they transact between each other, we would do that. But we don't participate in any of the authorizing of payments or anything at the consumer level.

Senator Tannas: What about to financial institutions in the United States? Would you be doing that or are you solely contained in the Canadian financial system?

Mr. Ferrabee: We would do the wire transfer as well.

Senator Tannas: Then, my financial institution, facilitated by you, is sending my payment somewhere. Is there any discussion anywhere about where it goes and how you could get it back if it turns out a day later that it's fraud?

transféré d'une institution financière canadienne à une institution financière américaine ne puisse pas se volatiliser?

Autrement dit, dans le cadre de cette discussion, est-ce qu'on se penche sur des moyens pour récupérer cet argent pour les Canadiens ordinaires?

Je sais qu'il faut y aller au cas par cas. Nous avons appris que cela se produit probablement des millions de fois. J'ai été victime de cela dans le milieu des affaires, et mon ordinateur a aussi été piraté; j'ai dû payer beaucoup d'argent, et on m'a seulement répondu : « C'est dommage. Vous avez perdu votre argent. »

Or, n'êtes-vous pas les mieux placés pour trouver des façons de récupérer cet argent ou d'endiguer ce flot? Y a-t-il des gens qui se penchent là-dessus, ou est-ce qu'on s'intéresse seulement aux menaces à grande échelle qui pèsent sur les grandes banques, sur le secteur hydroélectrique, et cetera? C'est un aspect tout aussi important, mais ne devrait-on pas se pencher sur les deux aspects?

M. Ferrabee : Je vais tenter de répondre le premier et de ne pas vous décevoir. En tant qu'infrastructure du marché financier, Paiements Canada va plus en profondeur que cela. Par exemple, nous nous occupons des échanges entre les institutions financières, qui constituent un très petit groupe. Comme ce sont ces institutions qui interagissent avec les clients, ce sont elles qui s'occupent des consommateurs, et l'ACFC est l'organisme qui défend les Canadiens dans les dossiers qui touchent les questions financières et les consommateurs de services financiers.

Nous ne nous occupons pas de cet échelon du système de paiement. Que nous ayons ou non un avis sur la question, Paiements Canada est une infrastructure dont le champ d'activité, aussi important soit-il, est limité et ne couvre pas la consommation.

Le sénateur Tannas : Si j'envoie un paiement, il ne passe pas du tout par votre infrastructure.

M. Ferrabee : Il sera traité par nos membres — les banques —, puis, finalement, par notre infrastructure lors des transactions entre les banques. Cependant, nous ne participons pas à l'autorisation des paiements ou aux processus à l'échelle du consommateur.

Le sénateur Tannas : Qu'en est-il des institutions financières aux États-Unis? Vous occupez-vous de cela ou seulement des institutions qui font partie du système financier canadien?

M. Ferrabee : Nous nous occupons également des virements.

Le sénateur Tannas : Alors, mon institution financière se sert de votre infrastructure pour envoyer mon paiement quelque part. Y a-t-il des gens, quelque part, qui se demandent où va cet argent et comment le récupérer si on s'aperçoit, le lendemain, que le paiement a été obtenu frauduleusement?

Mr. Kyle: A wire transfer goes over a separate network called the SWIFT network and the financial institutions are participants. Drawing upon my previous experience before Payments Canada, the ability to recall payments in the case of fraud is largely in the remit of the financial institutions themselves and their ability to leverage the relationships they have with their counterparts.

To the point of a previous panel that was here as part of this study, the difficulty in finding these perpetrators and prosecuting them is the inter-jurisdictional nature of the crime itself, which I think refers to the first part of your question.

There are two parts to your question. There's complexity in finding the perpetrators and prosecuting them from a jurisdictional point of view, and the second part was about redress for the consumer. That's largely handled by the retail financial institution that has some ability to claw back payments that may have been done fraudulently, or recompense the victim in the scenario.

I hope that answers some of your questions, but it's outside of the scope and realm of what we do in Payments Canada.

The Chair: These are great questions. Keep them for tomorrow, when we have the Canadian Chamber of Commerce and MasterCard. The interest of the consumer is very important.

Senator Wetston: A general question: The Bank for International Settlements has done a lot of working on financial market infrastructure. Have they done anything recently to guide your particular work in the area of cyber attacks or cybersecurity risk?

Mr. Ferrabee: We work with the Bank of Canada on that. It's very clear we work together in interpreting those and applying them to our context.

Mr. Kyle: There's one particular document I think was in our briefing note at the beginning, which identifies a standard to which we adhere, and it is the *Guidance on cyber resilience for financial market infrastructures*. That guidance was published by the Bank for International Settlements and there were participants from the Bank of Canada that helped contribute the content.

Senator Wetston: You don't directly participate?

Mr. Kyle: We didn't participate in the crafting of the document but we adhere to the principles identified in it.

Senator Wetston: Can you tell me whether you think there are more vulnerabilities, if any, in payments versus clearing and settlement in the large value transfer system? Do you have any

M. Kyle : Les virements passent par un réseau séparé, le réseau SWIFT, dont les utilisateurs sont les institutions financières. En me fondant sur l'expérience que j'ai acquise avant d'être à Paiements Canada, je dirai que la possibilité de révoquer des paiements en cas de fraude relève en grande partie des institutions financières et de leur pouvoir de négociation avec leurs homologues.

Pour revenir à un argument soulevé pendant une discussion précédente dans le cadre de cette étude, la difficulté à trouver ces délinquants et à les poursuivre en justice découle du fait que le crime en question touche plus d'un État. Je crois que cela répond à la première partie de votre question.

Votre question porte sur deux aspects : la difficulté de trouver les délinquants et de les poursuivre en justice, et les recours des consommateurs. Ce sont principalement les institutions financières de détail qui sont en mesure de recouvrer des paiements qui pourraient avoir été obtenus frauduleusement ou d'indemniser la victime du crime en question.

J'espère avoir répondu à quelques-unes de vos questions, mais ce sont là des responsabilités qui ne font pas partie du champ d'activité de Paiements Canada.

Le président : Ce sont d'excellentes questions. Gardez-les pour demain, lorsque nous allons entendre des représentants de la Chambre de commerce du Canada et de Mastercard. L'intérêt du consommateur est un aspect très important.

Le sénateur Wetston : J'ai une question générale. La Banque des règlements internationaux a fait beaucoup de travail à l'égard des infrastructures du marché financier. A-t-elle fait quelque chose récemment pour orienter votre travail en ce qui a trait aux cyberattaques ou aux menaces à la cybersécurité?

M. Ferrabee : Nous travaillons avec la Banque du Canada dans ce dossier. Il va de soi que nous travaillons de concert afin d'interpréter les résultats de ces travaux et de les adapter à notre situation.

M. Kyle : Il existe un document en particulier qui, si je ne m'abuse, a été mentionné dans notre déclaration préliminaire, et qui établit une norme à laquelle nous adhérons : le *Document d'orientation sur la cyberrésilience pour les infrastructures des marchés financiers*. Ce document a été publié par la Banque des règlements internationaux, et des gens de la Banque du Canada ont contribué à l'élaboration du contenu.

Le sénateur Wetston : Vous n'y participez pas directement?

M. Kyle : Nous n'avons pas participé à l'élaboration du document, mais nous adhérons aux principes qui y sont définis.

Le sénateur Wetston : Selon vous, y a-t-il d'autres composantes vulnérables au sein du système de transfert de paiements de grande valeur, que ce soit à l'échelle des

sense of where the vulnerabilities might be or what might be more accessible from the point of view of a cyber attack?

Mr. Kyle: For reasons that perhaps are obvious, we don't typically discuss security configurations or components. While we have a sense of where things are stronger or weaker, we don't discuss that but would disclose them to authorized parties if appropriate.

Senator Wetston: I guess what's important is if there are differences and you have identified what they are, you obviously don't want to recognize them in case there are cyber criminals who want to know that as well, for apparent reasons. But is there a difference? If there is a difference, are you aware of it, and do you take whatever action is appropriate to deal with that? Can you answer that?

Mr. Ferrabee: There is a difference, partly on scale, the number of participants and the level of trust in the system. The smaller you are, the higher level of trust. We are quite small and have a small number of members, so we have a high degree of trust. That risk gets higher as you get further out.

Senator Wetston: I look at it generally in this way that everything in our society is becoming more digitized. I don't know what we will call ourselves in 10 years but we may not call ourselves human beings. We may be robots entirely digitized and running on AI systems.

You will probably agree with me that today you can gather enough data for analysis or for whatever use you may want to make of it. Whereas five, six or seven years ago, it would have taken you a month to gather the same data, which makes that data more accessible to cyber attacks, I would think.

Given that circumstance with AI and big data — or whatever it's called; I can't recall the exact technology term for it — do you have concerns around the amount of available and potentially important data that can be accessed and organized in a day, rather than taking a considerable amount of time, and make it more available for attacks?

Mr. Ferrabee: I will address it at a more general level. There is an acceleration of capability and a broadening of technologies happening, and the work for us is being current. We invest significantly in ensuring we are up to date and are also tracking what's coming and what the impact is.

paiements, de la compensation ou des règlements? Avez-vous une idée des composantes qui pourraient être vulnérables ou exposées davantage à une cyberattaque?

M. Kyle : Pour des raisons qui peuvent sembler évidentes, nous n'avons pas l'habitude de discuter des structures ou des composantes de sécurité. Même si nous avons une idée des composantes qui sont plus fortes ou plus faibles, nous n'en discutons pas, mais nous signalons les lacunes aux autorités concernées au besoin.

Le sénateur Wetston : Je suppose que, ce qui importe, c'est de savoir s'il y a des écarts entre les systèmes, et si vous les avez cernés, même si, bien sûr, vous ne voudriez pas les exposer au cas où des cybercriminels s'intéresseraient également à cette information, pour des raisons évidentes. Cependant, y a-t-il des écarts? Si c'est le cas, êtes-vous au courant, et prenez-vous les mesures qui s'imposent pour y remédier? Pouvez-vous répondre à cette question?

M. Ferrabee : Il y a bel et bien des écarts, notamment selon l'échelle, le nombre de participants et la confiance à l'égard du système. Plus le système est petit, plus le niveau de confiance est élevé. Notre système est très petit et dessert un petit nombre de membres, ce qui fait que le niveau de confiance est élevé. Le risque augmente avec la taille du système.

Le sénateur Wetston : Je considère les choses en fonction du fait que, de façon générale, notre société se numérise de plus en plus. Je ne sais pas quel terme sera employé dans 10 ans, mais nous pourrions ne plus nous désigner comme des humains. Nous pourrions être des robots dont toutes les activités seraient numérisées et gérées par des systèmes d'intelligence artificielle.

Vous conviendrez sans doute que, de nos jours, on peut recueillir suffisamment de données en une journée pour faire une analyse ou n'importe quoi d'autre, alors que, il y a cinq ou six ans, il aurait fallu des mois pour recueillir les mêmes données. À mon sens, cela rend les données plus vulnérables aux cyberattaques.

Dans le contexte de l'intelligence artificielle et des mégadonnées — ou quel que soit le terme employé; je ne me souviens plus du terme exact pour désigner cette technologie —, craignez-vous que le fait de pouvoir recueillir et structurer un grand volume de données potentiellement importantes en une journée plutôt que sur une longue période rende ces données plus vulnérables à des attaques?

M. Ferrabee : Je vais tenter de répondre de façon générale. On observe actuellement une accélération des capacités et une utilisation plus vaste des technologies, ce qui nous force à rester à jour. Nous faisons des investissements considérables pour mettre nos méthodes à jour, et nous sommes à l'affût des nouvelles réalités et de leurs conséquences.

I think the short answer is yes, we are aware. It is more sophisticated and, as a result, carries more risk and that forces a greater vigilance on our side.

Senator Wetston: Is it more accessible?

Mr. Ferrabee: Because there is more of it? Possibly. We design our systems such that those conditions don't compromise us further. We would be aware of that as a constraint.

Senator Wetston: Do you believe, in your experience and what you do, obviously, that cyberattackers are as sophisticated and as capable as you are?

Mr. Ferrabee: Absolutely.

Senator Wetston: Are they more capable?

Mr. Ferrabee: It's very possible.

Senator Wetston: I guess that's the concern.

Mr. Ferrabee: That's the concern, and we don't know to what extent we are there but we keep at it.

[Translation]

Senator Dagenais: I would like to thank our guests.

I want to come back to the culture of secrecy of certain organizations and even of some of the institutions involved. To what extent does this culture of secrecy threaten to delay decisions in the event of a cyber attack, and what are the consequences?

[English]

Mr. Ferrabee: That's a very good question. It's hard to know how secret colleagues or partners are being.

The challenge we have and we try to articulate here is as we move more quickly, the collaborative nature becomes more important and it is dependent on not hiding secrets.

We are trying to adjust that as well, which is almost more at a relational level to make things more transparent, and we are aware of that as an issue to address in the partner relationships we have.

Je pense que la réponse courte est que nous sommes effectivement conscients de ces risques. Les méthodes sont plus avancées, ce qui entraîne plus de risques et nous force donc à faire preuve d'une plus grande vigilance.

Le sénateur Wetston : Les données sont-elles plus accessibles?

M. Ferrabee : Parce qu'elles sont plus nombreuses? C'est possible. Nous élaborons nos systèmes de manière à éviter que ces conditions nous rendent plus vulnérables. Nous sommes conscients de cette contrainte.

Le sénateur Wetston : Croyez-vous, toujours selon votre expérience et votre champ d'activité, évidemment, que les auteurs de cyberattaques ont des méthodes aussi avancées et efficaces que les vôtres?

M. Ferrabee : Tout à fait.

Le sénateur Wetston : Ont-ils des méthodes plus efficaces?

M. Ferrabee : C'est très possible.

Le sénateur Wetston : Je suppose que c'est ce qui nous inquiète.

M. Ferrabee : C'est ce qui nous inquiète, et nous ne savons pas dans quelle mesure nous sommes à la hauteur, mais nous persévérons.

[Français]

Le sénateur Dagenais : Merci à nos invités.

Je vais revenir sur la culture du secret qui caractérise certains organismes et même certaines institutions en cause. Dans quelle mesure cette culture du secret risque-t-elle de retarder la prise de décisions lors d'une cyberattaque, et quelles en sont les conséquences?

[Traduction]

M. Ferrabee : C'est une très bonne question. Il est difficile de connaître l'ampleur de cette culture du secret chez nos collègues ou nos partenaires.

Le problème que nous devons résoudre et que nous tentons d'expliquer ici, c'est que, étant donné la rapidité à laquelle les choses évoluent, la collaboration devient de plus en plus importante, et elle exige de ne pas avoir de secrets.

Nous essayons également de nous adapter à cet égard, et cela se reflète surtout dans les efforts que nous faisons pour rendre nos échanges plus transparents, et nous sommes conscients qu'il s'agit d'une difficulté avec laquelle nous devons composer dans nos relations avec nos partenaires.

[Translation]

Senator Dagenais: We know that financial institutions deal with their clients. Sometimes, for strategic reasons, they do not want to alert their clients or create a climate of suspicion, because that would be detrimental to the institution. Therefore, they cultivate a certain culture of secrecy.

It is important to quickly take matters in hand and notify the client, because if the client, for whatever reason, is not notified of what is happening, he or she may continue to put themselves in a highly critical situation.

[English]

Mr. Ferrabee: We would certainly not perpetuate secrecy in the event that something came to our attention or awareness. We would not perpetuate or in any way restrict the transparency for those reasons. If we are not aware of it, it becomes hard for us to know. To the extent that we can become aware through our systems, then we would act on that.

[Translation]

Senator Dagenais: Would you like to add something, Mr. Kyle?

Mr. Kyle: Yes, thank you.

[English]

When consumers are affected through cyber fraud or some malicious act that impacts them, there is recourse through the process with their financial institution. And there are changes coming in the regulatory regime under PIPEDA that would require breach notification. Those changes will increase the transparency of material breaches across the country.

Some jurisdictions, Alberta for example — and I believe Quebec, but I'm not sure on that — has a breach notification requirement. For those consumers in those jurisdictions, they can look to their Privacy Commissioners for information about breaches, even in the financial sector if their personal information has been so compromised.

That's what happens on the retail side of banking with respect to consumers. Our community that connects into our systems and works to transfer funds is much smaller. With the banking community itself, we have strong relationships and so the level of trust, the interaction and the information sharing is much higher in our space. I wanted to clarify that distinction between who our stakeholders are directly and what happens with the consumer in the retail financial system.

[Français]

Le sénateur Dagenais : On sait que les institutions financières font affaire avec leur clientèle. Parfois, pour des raisons stratégiques, elles ne veulent pas alerter leurs clients ou créer un climat de suspicion, car cela pourrait nuire à l'institution. On peut donc cultiver une certaine culture du secret.

Il est important de prendre rapidement les choses en main et d'aviser le client, car si ce dernier, pour quelque raison que ce soit, n'est pas avisé de ce qui se passe, il peut continuer à se mettre dans une position très critique.

[Traduction]

M. Ferrabee : Nous n'allons certainement pas maintenir le secret si nous prenons connaissance d'un problème. Nous n'allons pas maintenir le secret ou restreindre le niveau de transparence pour ces raisons. Si nous ne sommes pas conscients du problème, il est difficile pour nous de le cerner. Si nous pouvons cerner un problème par l'entremise de nos systèmes, nous allons prendre les mesures nécessaires.

[Français]

Le sénateur Dagenais : Voudriez-vous ajouter quelque chose, monsieur Kyle?

M. Kyle : Oui, merci.

[Traduction]

Les consommateurs victimes de cyberfraude ou de gestes malveillants ont des recours auprès de leur institution financière. Par ailleurs, des modifications seront apportées prochainement au régime de réglementation au titre de la LPRPDE afin d'exiger la publication d'avis au sujet des atteintes à la sécurité. Ces modifications permettront d'accroître la transparence à l'égard des graves atteintes à la sécurité partout au pays.

Dans certaines provinces, dont l'Alberta — je crois que c'est aussi le cas au Québec, mais je n'en suis pas sûr —, on exige la publication d'avis sur les atteintes à la sécurité. Les consommateurs de ces provinces peuvent s'adresser au commissaire à la protection de la vie privée de leur province afin d'obtenir de l'information sur ces atteintes à la sécurité, même dans le secteur financier, afin de savoir si leurs renseignements personnels ont été compromis.

Voilà ce qui se passe entre les établissements bancaires de détail et les consommateurs. Dans notre cas, le nombre d'intervenants qui se connectent à nos systèmes et qui transfèrent des fonds est beaucoup plus limité. Avec le secteur bancaire comme tel, nous entretenons des liens étroits, ce qui signifie que, dans notre milieu, le niveau de confiance, d'interaction et d'échange de renseignements est beaucoup plus élevé. Je tenais à établir la distinction entre notre façon d'interagir avec les

[Translation]

Senator Dagenais: I have a more specific question. Do you have an idea of the number of persons that may be involved in fighting cyber attacks?

[English]

Mr. Ferrabee: At Payments Canada?

[Translation]

Senator Dagenais: Yes, among others.

[English]

Mr. Ferrabee: We wouldn't specify the number of people we have and the resources we are deploying on it, but I assure you it's material.

[Translation]

Senator Dagenais: Thank you very much.

[English]

The Chair: I want to thank you both very much. This has been extremely helpful to us. We are trying to broaden our understanding, and you have been very helpful with that today. We are indebted to you.

(The committee adjourned.)

intervenants de notre milieu et la façon dont le consommateur interagit avec le système financier de détail.

[Français]

Le sénateur Dagenais : J'ai une question un peu plus pointue : avez-vous une idée du nombre de personnes qui peuvent être impliquées dans la lutte contre les cyberattaques?

[Traduction]

M. Ferrabee : À Paiements Canada?

[Français]

Le sénateur Dagenais : Oui, entre autres.

[Traduction]

M. Ferrabee : Nous n'allons pas préciser le nombre de personnes que nous employons et l'ampleur des ressources que nous déployons, mais je vous assure que les moyens sont considérables.

[Français]

Le sénateur Dagenais : Merci beaucoup.

[Traduction]

Le président : Je vous remercie infiniment tous les deux. Cette séance a été fort instructive pour nous. Nous essayons de nous renseigner davantage sur le sujet, et vous y avez beaucoup contribué aujourd'hui. Nous vous en sommes reconnaissants.

(La séance est levée.)

EVIDENCE

OTTAWA, Thursday, March 1, 2018

The Standing Senate Committee on Banking, Trade and Commerce met this day at 10:30 a.m. to study and report on issues and concerns pertaining to cyber security and cyber fraud; and study the present state of the domestic and international financial system.

Senator Douglas Black (*Chair*) in the chair.

[*English*]

The Chair: Good morning and welcome, colleagues and members of the general public, who are following today's proceedings of the Standing Senate Committee on Banking, Trade and Commerce either here in the room or listening via the Web.

My name the Doug Black, I am a senator from Alberta and I have the privilege of chairing this committee. I would ask my colleagues if they would introduce themselves, please.

Senator Tannas: Scott Tannas from Alberta.

[*Translation*]

Senator Dagenais: Jean-Guy Dagenais from Quebec.

[*English*]

Senator Wetston: Howard Wetston, Ontario.

Senator Stewart Olsen: Carolyn Stewart Olsen, New Brunswick.

The Chair: Thank you all very much for being here.

We are also very ably served by our clerks and analysts.

Today is the sixth meeting on our study on issues and concerns pertaining to cybersecurity and cyberfraud, including cyber threats to Canada's financial and commercial sectors, the current state of cybersecurity technologies and cybersecurity measures and regulations in Canada and abroad.

The second portion of our meeting will focus on our general mandate, which is the present state of the domestic and international financial system.

For the first section of our hearing, I am pleased to welcome Scott Smith, Director, Intellectual Property and Innovation Policy at the Canadian Chamber of Commerce; as well as Robert W. Gordon, Executive Director of the Canadian Cyber Threat Exchange; and Ron Green, Chief Security Officer at MasterCard.

TÉMOIGNAGES

OTTAWA, le jeudi 1^{er} mars 2018

Le Comité sénatorial permanent des banques et du commerce se réunit aujourd'hui, à 10 h 30, afin d'étudier, pour en faire rapport, les questions et préoccupations relatives à la cybersécurité et à la cyberfraude, et d'étudier la situation actuelle du régime financier canadien et international.

Le sénateur Douglas Black (*président*) occupe le fauteuil.

[*Traduction*]

Le président : Bonjour et bienvenue à mes collègues de même qu'aux membres du grand public présents dans la salle ou qui suivent les délibérations du Comité sénatorial permanent des banques et du commerce d'aujourd'hui sur le Web.

Je m'appelle Doug Black. Je suis un sénateur de l'Alberta et j'ai le privilège de présider ce comité. Je demanderais à mes collègues de se présenter.

Le sénateur Tannas : Scott Tannas, de l'Alberta.

[*Français*]

Le sénateur Dagenais : Jean-guy Dagenais, du Québec.

[*Traduction*]

Le sénateur Wetston : Howard Wetston, de l'Ontario.

La sénatrice Stewart Olsen : Carolyn Stewart Olsen, du Nouveau-Brunswick.

Le président : Je vous remercie de votre présence.

Nous profitons également des excellents services de nos greffiers et analystes.

Aujourd'hui, nous tenons notre sixième réunion en vue d'étudier les questions et préoccupations relatives à la cybersécurité et à la cyberfraude, y compris les menaces cybernétiques contre les secteurs financier et commercial du Canada, la situation actuelle relative aux technologies de cybersécurité, et les mesures et règlements en matière de cybersécurité au Canada et à l'étranger.

La deuxième partie de notre réunion portera sur notre mandat général, soit la situation actuelle du régime financier canadien et international.

Pour la première partie de notre séance, c'est avec plaisir que nous recevons Scott Smith, qui est directeur de la propriété intellectuelle et de la politique d'innovation à la Chambre de commerce du Canada, Robert W. Gordon, qui est directeur

We have a very informed and distinguished panel, and we look forward to learning from you. Each of you is invited to make a presentation no longer than five minutes, and from there we will go to questions. Gentlemen, thank you for being here.

Mr. Gordon, the floor is yours.

Robert W. Gordon, Executive Director, Canadian Cyber Threat Exchange: Thank you, Mr. Chair and members of the committee, for the opportunity to address the issue of cyber-threats to Canada's financial and commercial sectors and the security measures in place to try to mitigate those threats.

As this is the first time someone from the Canadian Cyber Threat Exchange, or CCTX, has had the privilege of appearing before the committee, I will take the opportunity to describe why the CCTX was created and the role it plays in trying to assist the private sector to mitigate the risks posed by cyber-threats.

Approximately three years ago, the idea of creating a CCTX to facilitate the sharing of cyber-threat information was considered by a group of Canadian chief executive officers. They observed that knowledge about cyber-threats should not be a competitive issue among companies; they should all operate on the basic understanding of the cyber-threat they are facing. Companies can then even compete on the basis of the products and services they offer.

In December 2015, the CCTX was founded by nine companies which provided the initial funding: Air Canada, Bell Canada, Canadian National Railway, Hydro One Networks Inc., Manulife Financial, Royal Bank of Canada, TD Bank Group, TELUS and TransCanada Corporation. Today, the CCTX has grown to include members from 11 financial institutions, and industry sectors including transportation, telecommunications, energy, retail, professional services and entertainment.

There are several reasons why sharing cyber-threat information is important. Sharing leverages the knowledge of others and makes the cost of an attack more expensive. It enriches the cyber-threat information held by companies, making it more actionable. Timely, actionable information provides the means to harden cyberdefences. Sharing information is cost-effective; individual companies don't have to do all the analysis themselves. Sharing is one way of also helping to protect clients and the corporate supply chain. The bottom line: cybersecurity is a team sport.

général de l'Échange canadien de menaces cybernétiques, et Ron Green, qui est chef de la sécurité pour MasterCard.

Nous recevons un groupe de témoins éclairés et distingués; nous avons hâte de vous entendre. Nous invitons chacun d'entre vous à présenter un exposé d'au plus cinq minutes; nous passerons ensuite aux questions. Messieurs, nous vous remercions d'être ici aujourd'hui.

Monsieur Gordon, vous avez la parole.

Robert W. Gordon, directeur général, Échange canadien de menaces cybernétiques : Merci, monsieur le président, mesdames et messieurs les membres du comité, de me donner l'occasion d'aborder la question des menaces cybernétiques contre les secteurs financier et commercial du Canada, et des mesures de sécurité en place pour atténuer ces menaces.

Comme il s'agit de la première fois qu'un représentant de l'Échange canadien de renseignements sur les menaces cybernétiques, ou ECMC, a le privilège de témoigner devant le comité, je vais profiter de l'occasion pour expliquer pourquoi l'ECMC a été créé et le rôle qu'il joue en vue d'aider le secteur privé à atténuer les risques associés aux menaces cybernétiques.

Il y a environ trois ans, un groupe de dirigeants principaux canadiens a étudié la possibilité de créer l'ECMC pour faciliter l'échange de renseignements sur les menaces cybernétiques. Ils ont fait valoir que les connaissances au sujet des cybermenaces ne devaient pas être l'objet d'une concurrence entre les entreprises et que toutes les entreprises devraient avoir une compréhension de base à l'égard des menaces cybernétiques auxquelles elles sont confrontées. Les sociétés pourront ensuite se livrer une concurrence égale pour les produits et services qu'elles offrent.

En décembre 2015, l'ECMC a été créé par neuf sociétés qui ont offert un financement initial : Air Canada, Bell Canada, la Compagnie des chemins de fer nationaux, Hydro One Networks Inc., la Financière Manuvie, la Banque Royale du Canada, le Groupe Banque TD, TELUS et la Société TransCanada. Aujourd'hui, l'ECMC compte la participation de 11 institutions financières et des membres de divers secteurs comme le transport, les télécommunications, l'énergie, le commerce de détail, les services professionnels et le divertissement.

Les renseignements sur les menaces cybernétiques sont importants pour plusieurs raisons. L'échange de renseignements nous permet de miser sur les connaissances des autres et rend les attaques plus coûteuses. Il permet d'enrichir les renseignements sur les menaces cybernétiques consignés par les entreprises, ce qui les rend plus exploitables. Les renseignements opportuns et exploitables nous permettent de renforcer notre cyberdéfense. L'échange de renseignements est rentable, puisque les entreprises n'ont pas à faire l'analyse elles-mêmes. L'échange permet également de protéger les clients et la chaîne

The CCTX is a not-for-profit organization with two mandates. First, it serves as a cyber-threat information sharing hub. Second, it enables collaboration among member companies in countering cyber-threats. The CCTX is unique in that it represents all sectors and all sizes of companies.

The CCTX information sharing hub operates by receiving cyber-threat information from member companies and will shortly be receiving information from federal government departments and threat data feeds, which will be purchased from commercial vendors. Participating companies provide what are described as indicators of compromise, which is unusual cyber activity detected on their networks.

The information provided by the member companies is anonymized; there is no attribution as to which company provided the information and it contains no personal information.

CCTX analysts review the information and prepare a variety of reports. Some are tactical, relating to attacks under way, and some are of a more strategic nature, suitable for more business decision-making. In its first year of operation, the CCTX issued over 1,000 cyber reports.

Information sent to and received from the CCTX operations centre can be processed in a machine-readable format. The objective is to disseminate the information as quickly as possible so it can be incorporated into the defences of participating organizations. To be useful, information must be actionable. To be actionable, it must be timely and contextually relevant.

The CCTX's collaboration mandate provides cybersecurity professionals with the ability to exchange best practices and ideas. Exchanges occur within what we call communities of interest and communities of trust.

Communities of interest operate across industry sectors. Topics include trends in ransomware attacks, new technologies and data loss prevention. The exchanges occur in a variety of forms, including monthly conference calls, during which cybersecurity experts talk about the latest developments. The CCTX secure portal also has compartments where companies can post information and exchange comments on cybersecurity developments.

d'approvisionnement des entreprises. En somme, la cybersécurité est un sport d'équipe.

L'ECMC est un organisme à but non lucratif qui a deux mandats : d'abord, il agit à titre de centre d'échange de renseignements sur les menaces cybernétiques; ensuite, il permet aux sociétés membres de collaborer à la lutte contre les menaces cybernétiques. L'ECMC est unique puisqu'il représente tous les secteurs et les entreprises de toutes les tailles.

Le centre d'échange de renseignements de l'ECMC permet aux entreprises membres d'échanger des renseignements sur les menaces cybernétiques. Bientôt, il recevra des renseignements des ministères du gouvernement fédéral de même que des sources de données sur la menace, qui seront achetées à des fournisseurs commerciaux. Les sociétés participantes transmettent ce que l'on appelle les indicateurs de compromission, c'est-à-dire des cyberactivités inhabituelles détectées sur leurs réseaux.

Les renseignements transmis par les sociétés membres sont ensuite anonymisés : il est impossible d'associer les renseignements à une entreprise et il n'y a aucun renseignement personnel.

Les analystes de l'ECMC examinent les renseignements et préparent divers rapports connexes. Certains rapports sont de nature tactique et portent sur les attaques qui se préparent, et d'autres rapports sont plutôt de nature stratégique, pour aider les entreprises à prendre des décisions. Au cours de sa première année d'activité, l'ECMC a publié plus de 1 000 rapports.

Les renseignements envoyés et reçus par le centre des opérations de l'ECMC peuvent être traités selon un format lisible à la machine. L'objectif consiste à diffuser l'information le plus rapidement possible de sorte que les organisations participantes puissent s'en servir à des fins de défense. Pour être utiles, les renseignements doivent être exploitables. Pour être exploitables, ils doivent être opportuns et pertinents sur le plan contextuel.

Le mandat de collaboration de l'ECMC offre aux professionnels de la cybersécurité la possibilité d'échanger les meilleures pratiques et leurs idées. Les échanges se font dans ce que nous appelons des communautés d'intérêt et des communautés de confiance.

Les communautés d'intérêt comptent des membres des divers secteurs de l'industrie. On y parle notamment d'attaques de rançongiciels, des nouvelles technologies et de la prévention de la perte des données. Les échanges se font selon diverses formes, notamment par l'entremise de téléconférences mensuelles, au cours desquelles les experts en matière de cybersécurité parlent des derniers développements. Le portail sécurisé de l'ECMC contient également des compartiments où les sociétés peuvent publier des renseignements et échanger des commentaires sur les développements en matière de cybersécurité.

Communities of trust are established to facilitate collaboration among a small number of companies where there is either some particular sensitivity to the information being exchanged, or the nature of the exchange wouldn't be of interest to the broader group. A community of trust is currently operating with some banks and telecommunications companies who are examining specific cybersecurity threats.

Most of the collaboration occurs within the virtual environment. We also provide a physical space in our operations centre where cybersecurity professionals can meet in person to collaborate on solutions to current problems.

In addition, the CCTX hosts collaboration events at various locations around the country. These half-day events feature experts addressing a range of discussions, everything from new cybersecurity legislation to how artificial intelligence can enhance cybersecurity and the latest techniques used by cyber attackers.

The CCTX is preparing to receive information from two sources in the federal government: the Canadian Cyber Incident Response Centre in Public Safety Canada and the Communications Security Establishment. CCIRC and CSE help support Canada's critical infrastructure operators. Working in partnership with the CCTX, they extend that support to a much broader constituency.

The CCTX benefits from the expertise of permanent invitees to meetings of the board of directors. These include Public Safety Canada, the Communications Security Establishment, the Business Council of Canada and academia. Currently, Benoît Dupont from Smart Cybersecurity Network, who previously appeared before this committee, is the representative from academia.

In conclusion, the initial focus of the CCTX has been on growing the membership of large organizations and providing them with products and services. The next phase will be the development of cybersecurity products and services tailored to meet the cybersecurity needs of small- and medium-sized companies. We are exploring expanded partnership opportunities with academia to help grow the number of cybersecurity professionals that are in desperately short supply in Canada and to enable cybersecurity research that will work to the benefit of all Canadians.

Thank you very much. I look forward to your questions.

The Chair: Very good presentation. Thank you very much, Mr. Gordon. Mr. Smith, please go ahead.

Les communautés de confiance sont mises sur pied afin de faciliter la collaboration entre quelques entreprises lorsque les renseignements échangés sont de nature particulièrement sensible ou lorsque les échanges risquent de ne pas intéresser l'ensemble des membres. Une communauté de confiance a été mise sur pied et compte la participation de banques et entreprises de télécommunications qui étudient certaines menaces cybernétiques particulières.

La majeure partie de la collaboration se fait dans l'environnement virtuel. Nous offrons également un espace physique dans notre centre des opérations où les professionnels de la cybersécurité peuvent se réunir en personne dans le but de trouver des solutions aux problèmes actuels.

De plus, l'ECMC organise des événements de collaboration à divers endroits au pays. Au cours de ces événements d'une demi-journée, des experts viennent discuter d'un éventail de sujets, qu'il s'agisse des nouvelles lois en matière de cybersécurité, de la façon dont l'intelligence artificielle peut améliorer la cybersécurité ou des dernières techniques utilisées par les auteurs de cyberattaques.

L'ECMC se prépare à recevoir des renseignements de deux sources au gouvernement fédéral : le Centre canadien de réponse aux incidents cybernétiques de Sécurité publique Canada et le Centre de la sécurité des télécommunications. Les deux centres appuient les exploitants d'infrastructures essentielles du Canada. En collaborant avec l'ECMC, ils élargissent ce soutien et l'offrent à un plus grand nombre d'organisations.

L'ECMC profite de l'expertise des invités permanents aux réunions du conseil d'administration, notamment des universitaires et des représentants de Sécurité publique Canada, du Centre de la sécurité des télécommunications et du Conseil canadien des affaires. À l'heure actuelle, Benoît Dupont, du Réseau intégré sur la cybersécurité, qui a déjà témoigné devant le comité, est le représentant du milieu universitaire.

Pour conclure, l'objectif premier de l'ECMC était d'attirer de grandes organisations et de leur offrir des produits et services. La prochaine étape visera à développer des produits et services en matière de cybersécurité conçus pour répondre aux besoins des petites et moyennes entreprises. Nous étudions les possibilités de partenariats élargis avec les universités afin d'accroître le nombre de professionnels de la cybersécurité, puisqu'il y a une importante pénurie en la matière au Canada, et de favoriser la recherche sur la cybersécurité, dont profiteront tous les Canadiens.

Merci beaucoup. C'est avec plaisir que je répondrai à vos questions.

Le président : Merci beaucoup, monsieur Gordon; c'était un très bon exposé. Monsieur Smith, allez-y, s'il vous plaît.

Scott Smith, Director, Intellectual Property and Innovation Policy, The Canadian Chamber of Commerce: Thank you, Senator Black and members of the committee, for the invitation to appear before you to talk about cybersecurity, something that's been near and dear to me for the last couple of years.

I am pleased to be here to represent the Canadian Chamber of Commerce. We are the largest business organization in Canada. We have a network of over 450 local chambers of commerce, which are all members of ours, that represent over 200,000 businesses of all sizes and all sectors of the economy and in all regions in Canada. My comments this morning are reflective of regular dialogue with those members.

Cybercrime is a catch-all term that describes a number of more specific transgressions accomplished by infiltrating computers across networks. Fraud in the form of identity theft or the spoofing of legitimate websites to lure customers is a pervasive problem. So is extortion in the form of ransomware. Destroying data or hardware is vandalism. Acquiring credit card numbers or leaking sensitive personal information for financial gain is theft. "Hacktivism" is any one of those crimes committed in the name of a cause. Then there is the more benign crime of trespassing, which is stopping for an unwelcome look at someone's computer.

Cybercrime costs everyone everywhere. Studies suggest that cyber attacks cost the global economy \$445 billion. In Canada, the number of businesses experiencing losses from cybercrime is increasing. The Ponemon Institute last year surveyed 24 companies across all sectors and noted the average cost of a data breach is \$6 million. The average cost per record of a breach is \$258. And the average number of records breached in 2016 was 20,456.

We've seen some large, very public breaches over the last few years. In 2013, the Yahoo breach impacted more than 3 billion people. The Equifax breach last year affected far fewer, only 143 million, but that has shaken the public trust because this is the company that monitors your credit after a breach.

The most expensive breach ever was MyDoom over a decade ago. That was \$38.5 billion in damage.

Cyberbreaches impact businesses large and small, but we only hear about the large ones, the household names. I want to talk about the small businesses in Canada and how they are impacted.

Scott Smith, directeur, Propriété intellectuelle et politique d'innovation, Chambre de commerce du Canada : Sénateur Black, mesdames et messieurs les membres du comité, merci de l'invitation à comparaître pour traiter des questions relatives à la cybersécurité, un enjeu qui est au centre de mes préoccupations ces deux ou trois dernières années.

Je suis heureux d'être ici pour représenter la Chambre de commerce du Canada, le plus grand organisme de gens d'affaires au Canada. Notre réseau regroupe plus de 450 chambres de commerce représentant 200 000 entreprises de toutes les tailles dans tous les secteurs de l'économie et toutes les régions. Mes observations de ce matin seront représentatives de nos discussions régulières avec nos membres.

« Cybercriminalité » est un terme générique qui sert à décrire diverses intrusions plus précises découlant de l'infiltration d'ordinateurs branchés en réseau. La fraude, sous forme de vol d'identité ou d'usurpation de sites web légitimes pour harponner les clients, et l'extorsion, à l'aide de logiciels rançonneurs, sont des problèmes omniprésents. La destruction de données ou de matériel constitue du vandalisme, tandis que l'acquisition de numéros de carte de crédit ou la divulgation de renseignements personnels de nature délicate afin d'en tirer un profit financier constitue du vol. On appelle « hacktivisme » tout crime de cette nature commis au nom d'une cause. À cela s'ajoute le crime plus inoffensif de l'intrusion, par exemple une personne qui serait pour jeter un coup d'œil non sollicité sur l'ordinateur d'une autre personne.

La cybercriminalité a un coût pour tout le monde, dans toutes les sphères d'activité. Selon certaines études, la cybercriminalité devrait coûter quelque 445 milliards de dollars à l'économie mondiale. Au Canada, le nombre d'entreprises ayant subi des pertes causées par la cybercriminalité est en augmentation. Dans une étude réalisée l'an dernier auprès de 24 entreprises de tous les secteurs de l'économie, l'Institut Ponemon a évalué à 6 millions de dollars le coût moyen d'une fuite de données, pour un coût moyen de 258 \$ par dossier. En 2016, 20 456 dossiers en moyenne ont fait l'objet d'une brèche de sécurité.

D'importantes fuites très médiatisées ont eu lieu ces dernières années. En 2013, la brèche de sécurité Yahoo a touché plus de 3 milliards d'utilisateurs. La brèche de sécurité chez Equifax a touché beaucoup moins de gens, soit seulement 143 millions de personnes, mais cet incident a ébranlé la confiance du public, car ils touchaient l'entreprise chargée de la surveillance de votre crédit après une brèche.

L'incident le plus coûteux a été celui de MyDoom, il y a plus d'une décennie, qui a causé 38,5 milliards de dollars de dommages.

Les brèches informatiques touchent toutes les entreprises, grandes et petites, mais nous n'entendons parler que des cas qui touchent les grandes entreprises, les plus connues. Je tiens à vous

In Canada, 98 per cent of businesses have fewer than 100 employees, and 74 per cent have fewer than 10 employees. These small- and medium-sized businesses employ 10.5 million people in Canada, 90 per cent of private sector employees, a vital part of our economy.

They are the most vulnerable to exploitation from cybercriminals because they lack the financial and human resources to protect them effectively. The cybercriminals are organized and multi-layered. Ransomware is now sold as a service on the dark web.

The process is straightforward. You specify your bitcoin address to get the ransom, select the amount you want to collect from the ransom, anywhere between 0.01 BTC and a maximum of 1 BTC, and you get a nice piece of malicious software delivered to your inbox a few seconds later. Then you deploy it to whatever predetermined email list you choose. Once launched, that malware will encrypt files, and the unsuspecting mark will have to pay the ransom to get their files back, or at least, some of them will. The business model behind this is simple: The bad guys keep 10 per cent of the ransom; it's almost like a distribution network for ransomware.

This has happened recently to one of our local Chambers of Commerce in southwestern Ontario. They were attacked by ransomware—someone clicked on the wrong attachment. They were smart enough not to pay the ransom, but there was a significant cost in downtime, in IT consulting and in reputation, and there were some files lost forever due to the backup cycle. It will never be a perfect solution.

There are 3.5 million emails sent every second globally. One in 40 contains malicious software. The threat is real. We have to remember — and what I hope members of this committee will remember as policy-makers — that the businesses who are impacted by cybercrime are the victims. When we are crafting regulatory policy to protect personal information, the businesses that have been breached are required to report and make amends for those breaches, and they themselves are in crisis mode. A regulatory policy should be focused on the perpetrators of the crime.

The CIA considers three things when assessing threats: confidentiality, which means protecting and keeping your secrets, so espionage and data thefts are threats to confidentiality; availability, which means keeping your services running and giving administrators access to key networks and controls, so denial of service and data deletion attacks threaten

parler des petites entreprises canadiennes et des répercussions qu'elles subissent.

Au Canada, 98 p. 100 des entreprises comptent moins de 100 employés, et 74 p. 100 en ont moins de 10. Ces petites et moyennes entreprises emploient 10,5 millions de personnes au Canada, dont 90 p. 100 sont dans le secteur privé, un élément essentiel de notre économie.

Ces entreprises sont les plus vulnérables à l'exploitation par des cybercriminels, étant donné leur manque de ressources financières et humaines pour se protéger efficacement. Les cybercriminels sont organisés et agissent sur plusieurs tableaux. Sur le Web invisible, les logiciels rançonneurs sont maintenant vendus en tant que service.

Le processus est simple. Il s'agit de donner une adresse Bitcoin pour le versement de la rançon, de fixer le montant de la rançon, qui peut être de n'importe quel montant entre 0,01 bitcoin et 1 bitcoin, au maximum. Ensuite, quelques secondes plus tard, un formidable logiciel malveillant vous est livré dans votre boîte de réception. Ensuite, vous le déployez à tous les destinataires d'une liste prédéterminée. Une fois lancé, le logiciel malveillant crypte des fichiers, et les innocentes cibles — ou du moins certaines d'entre elles — paient pour récupérer leurs fichiers. Le modèle d'affaires est très simple. Essentiellement, le criminel reçoit 10 p. 100 de la rançon. C'est pratiquement un réseau de distribution pour logiciels rançonneurs.

C'est d'ailleurs arrivé récemment à l'une de nos chambres de commerce membres du sud-ouest de l'Ontario. Elle a été touchée par une attaque au logiciel rançonneur; quelqu'un a cliqué sur la mauvaise pièce jointe. Ils ont eu l'intelligence de ne pas payer la rançon, mais les coûts ont été importants. On parle ici des coûts liés à l'arrêt des activités, aux services de TI et à l'atteinte à la réputation. En outre, certains fichiers ne pourront être récupérés, en raison du cycle de sauvegarde. Il n'y a pas de solution parfaite.

À l'échelle mondiale, 3,5 millions de courriels sont envoyés chaque seconde, et un courriel sur 40 contient un logiciel malveillant. La menace est réelle. Il convient de se rappeler — et j'espère que vous garderez cela à l'esprit, en tant que décideurs — que les entreprises touchées par la cybercriminalité sont des victimes. Dans les politiques de réglementation visant la protection des renseignements personnels, les entreprises qui ont été piratées sont tenues de le signaler et de réparer les torts, tandis qu'elles sont elles-mêmes en gestion de crise. Le cadre réglementaire devrait être axé sur les auteurs du crime.

Lorsqu'elle évalue les menaces, la CIA tient compte de trois aspects. Premièrement, la confidentialité, soit la capacité de protéger et de maintenir le secret. L'espionnage et le vol de données sont des menaces à la confidentialité. Deuxièmement, la disponibilité, c'est-à-dire le maintien des services et l'accès accordé aux administrateurs pour les réseaux et commandes clés.

your availability; and integrity, which means assessing whether the software and critical data within your networks and systems are compromised with malicious or unauthorized code and viruses and malware that compromise the integrity of the systems they infect.

Our focus at the Chamber of Commerce is how business needs to be aware of this triad, how cybersecurity is a vital risk-management exercise and how government can facilitate awareness and engagement and the steps companies can take to protect themselves.

Our report, *Cybersecurity in Canada: Some Practical Solutions to a Growing Problem*, which I think you have either a link or copy of, proposed a number of policy options the Government of Canada could undertake to provide leadership and resources for the business community to remain competitive.

We were pleased to see this week's budget announcement included a number of measures we outlined in our report. For instance, we asked for the consolidation of cybersecurity policy under one agency. Budget 2018 proposes to do that, adding \$155 million to the budget of CSE.

We asked for more focus on protecting critical infrastructure. Budget 2018 commits to that. We asked for more resources to combat cybercrime. Budget 2018 provides \$116 million to the RCMP to do that.

We asked for support for small business in combatting cyber threats. Budget 2018 allocates \$236 million to support a cybersecurity strategy that includes cybereducation and a cyber resilience certification program. We're close to the cybersecurity certification program proposed out of New Brunswick. We're hoping to make an announcement shortly that we will be helping to distribute that across the country and encouraging businesses to participate, but we were part of the development of that process. Hopefully, the government goes for that as part of the voluntary certification program.

The other thing we were hoping for in the budget, but did not see, was tax measures to make investments in cybersecurity network systems and software accelerate the speed to be able to write those off. You might want to consider that down the road. It will be welcome in the business community. We look forward

Les attaques par déni de service et la suppression des données menacent la disponibilité. Le troisième est l'intégrité; il s'agit de vérifier si les logiciels et les données critiques de vos réseaux et systèmes sont compromis avec des codes ou des bogues malveillants ou non autorisés. Les virus et les logiciels malveillants compromettent l'intégrité des systèmes qu'ils infectent.

La Chambre de commerce est axée sur la façon dont les entreprises doivent prendre conscience de cette trilogie, sur l'importance de la cybersécurité en tant qu'exercice vital de la gestion des risques, sur les mesures que peut prendre le gouvernement pour favoriser la sensibilisation et l'engagement et sur les mesures que peuvent prendre les entreprises pour se protéger.

Dans notre rapport intitulé *Cybersécurité au Canada : Solutions pratiques à un problème de taille*, dont nous vous avons fourni un exemplaire, ou un lien pour le consulter, nous proposons diverses options de politiques que le gouvernement du Canada pourrait mettre en place pour assurer un rôle de chef de file et offrir au milieu des affaires les ressources nécessaires pour maintenir sa compétitivité.

Nous avons été ravis de constater que le budget annoncé cette semaine comprenait diverses mesures que nous avons proposées dans notre rapport. Par exemple, nous avons demandé le regroupement des diverses politiques de cybersécurité au sein d'un seul organisme. Le budget de 2018 contient une proposition en ce sens, en bonifiant le budget du CST de 155 millions de dollars.

Nous avons demandé qu'on accorde plus d'attention à la protection des infrastructures essentielles, et le budget de 2018 comporte un engagement en ce sens. Nous avons demandé des ressources supplémentaires pour combattre la cybercriminalité, et le budget de 2018 accorde à la GRC 116 millions de dollars à cette fin.

Nous avons demandé un appui aux petites entreprises pour la lutte contre les cybermenaces. Le budget de 2018 prévoit 236 millions de dollars pour appuyer une stratégie en matière de cybersécurité comprenant de la formation et un programme de certification en cyberrésilience. Nous aurons bientôt mis en place un programme de certification en cybersécurité au Nouveau-Brunswick. Nous espérons pouvoir bientôt annoncer notre contribution au déploiement de ce programme dans l'ensemble du pays et ainsi encourager les entreprises à participer. Nous avons participé à l'élaboration de ce processus. Nous espérons que le gouvernement acceptera de jouer un rôle dans le programme de certification volontaire.

Dans le budget, nous souhaitons également voir des mesures fiscales permettant la radiation accélérée des investissements dans les systèmes et les logiciels réseau de cybersécurité, mais cette demande est restée lettre morte. Vous pourriez examiner cette solution pour l'avenir. Ce serait bien accueilli dans le

to working with the government of Canada as it crafts its cybersecurity strategy.

Thank you for your attention and I look forward to your questions.

Ron Green, Chief Security Officer, MasterCard: Good morning and thank you for the opportunity to be here today. My name is Ron Green, and I am the Chief Security Officer at MasterCard.

First and foremost, I want to praise the committee for launching this study. Cybersecurity is one of the greatest challenges governments and businesses are facing at the present time, with serious implications for national security, financial stability and consumer protection. Cybersecurity is a top global priority at MasterCard. At MasterCard, safety and security are foundational principles central to every part of our business in the innovative technology platforms and services we enable.

We know that secure products and services are essential to the trust our consumers, customers, cardholders, merchants and other partners place in us.

Let me contextualize that. As you probably know, MasterCard does not issue credit cards or have a direct relationship with consumers. That is the purview of the banks that issue our cards. MasterCard is a technology company, and we provide the network that allows consumers to use their MasterCard virtually anywhere in the world, more than 210 countries and territories, and have that transaction processed in seconds.

We operate the world's fastest payments processing network and connect 2.3 billion cardholders with tens of millions of merchants around the world. For us to provide value to banks, merchants and consumers that use our networking, we must provide safety and security. We cannot afford to have any interruptions in the operations of our network. When a bank issues our card, when a consumer takes the card out of his or her wallet, or when a merchant decides to accept MasterCard, each of those stakeholders needs to do so with the confidence that the network over which those payments will be made is reliable and resilient.

We have a solid record on that. The MasterCard network has layers of cyber defences designated to mitigate risk and protect it from being hacked. We are continually building resiliency to prevent service interruption. We at MasterCard are constantly investing in security. Over the last three years, we have invested over \$1 billion in reinforcing the cyber defences of our network and developing solutions to protect participants in the payments

milieu des affaires. Nous avons hâte de collaborer avec le gouvernement du Canada à l'élaboration de sa stratégie en matière de cybersécurité.

Je vous remercie de votre attention. C'est avec plaisir que je répondrai à vos questions.

Ron Green, chef de la sécurité, MasterCard : Bonjour. Je vous remercie de l'occasion de comparaître aujourd'hui. Je m'appelle Ron Green et je suis chef de la sécurité chez MasterCard.

Tout d'abord, je tiens à féliciter le comité d'avoir entrepris cette étude. La cybersécurité est l'un des plus grands défis auxquels sont confrontés les gouvernements et les entreprises à l'heure actuelle, ce qui a de graves répercussions pour la sécurité nationale, la stabilité financière et la protection des consommateurs. La cybersécurité est une priorité mondiale absolue chez MasterCard. La sécurité est un principe fondamental qui fait partie intégrante de nos activités dans les plateformes et services technologiques novateurs que nous offrons.

Nous savons que des produits et services sécurisés sont essentiels pour obtenir la confiance de nos consommateurs, de nos clients, de nos détenteurs de carte, de nos commerçants et d'autres partenaires.

Permettez-moi de fournir un peu de contexte. Comme vous le savez sans doute, MasterCard n'émet pas de carte de crédit ou n'a pas de relations directes avec les consommateurs. Les banques ont la responsabilité d'émettre nos cartes. Mastercard est une entreprise technologique, et nous offrons le réseau qui permet aux consommateurs d'utiliser leur MasterCard pratiquement n'importe où dans le monde, dans plus de 210 pays et territoires, et nous traitons les transactions en quelques secondes.

Nous exploitons le réseau de traitement des paiements le plus rapide au monde et relierons 2,3 milliards de détenteurs de cartes avec des dizaines de millions de commerçants dans le monde. Pour offrir de la valeur aux banques, les commerçants et les consommateurs qui utilisent notre réseautage, nous devons assurer une sécurité. Nous ne pouvons pas nous permettre des interruptions dans les opérations de notre réseau. Lorsqu'une banque émet notre carte, lorsqu'un consommateur sort la carte de son porte-feuille, ou qu'un commerçant décide d'accepter MasterCard, tous ces intervenants doivent avoir confiance que le réseau sera fiable et solide.

Nous avons un excellent bilan à cet égard. Le réseau de MasterCard a des niveaux de cyberdéfense pour atténuer les risques et protéger le réseau contre le piratage. Nous renforçons constamment la résilience du réseau pour éviter des interruptions de service. Chez MasterCard, nous investissons constamment dans la sécurité. Au cours des trois dernières années, nous avons investi plus de 1 milliard de dollars pour renforcer les

ecosystem — issuing banks, acquirers, merchants and cardholders. This has involved taking the lead in developing new payment and commerce ecosystem standards, which are constantly being revised with an eye to security. We are investing in innovation and enhancing our capabilities in house, acquiring cutting edge technology companies and nurturing our Start Path group of curated startups, connecting them with our issuing partners to grow their business.

There are five widely accepted elements essential for cybersecurity risk management. MasterCard operationalizes them in the following ways:

Identify: We are doing interesting things here, including MasterCard's identity check, which Canadian banks were among the first to commercialize. The priority is to authenticate the identity of the network users.

Protect: Here device security is critical. With a networked system, any device can be an entry point for a cyber attack. To this end, last year MasterCard acquired NuData Security, an innovative Canadian technology company that helps businesses prevent online and mobile fraud by using behavioural and biometric indicators. NuData enhances our capabilities, including preventing consumer device cyber attacks, account takeover and enabling intelligent friction.

Detect: Essentially stopping an attack before it begins. Here we are making major investments in artificial intelligence, including the recent acquisition of Brighterion, a global AI leader, which enhances our ability to detect sophisticated attacks. Brighterion's AI solutions help MasterCard find the proverbial needle in the haystack when it comes to sifting through massive quantities of data.

Respond: In order to respond effectively to threats, information sharing and collaboration among industry partners, financial institutions, the FS-ISAC are essential. In the United States, cyberemergency readiness teams, or CERTS, align with their counterparts in other countries, including Canada.

Recover: Like other industry leaders, MasterCard is continually building and improving resiliency plans to ensure our backup plans work if needed.

This includes a real time machine-to-machine automated means of responding. At a very high level, this is what we are doing.

cyberdéfenses de notre réseau et pour concevoir des solutions afin de protéger les participants dans l'écosystème des paiements — banques émettrices, acquéreurs, commerçants et détenteurs de carte. Il faut notamment prendre l'initiative d'élaborer de nouvelles normes en matière d'écosystèmes de paiements et de commerce, qui sont constamment révisées en tenant compte de la sécurité. Nous investissons dans l'innovation et nous renforçons nos capacités à l'interne, en faisant l'acquisition d'entreprises technologiques de pointe et en soutenant notre groupe Start Path de jeunes entreprises, en les mettant en lien avec nos partenaires émetteurs pour qu'elles puissent prendre de l'expansion.

Il y a cinq éléments généralement acceptés pour la gestion des risques en matière de cybersécurité. MasterCard les applique des façons suivantes :

Ciblage : nous faisons des choses intéressantes, notamment des vérifications d'identité, que les banques canadiennes ont été parmi les premières à commercialiser. La priorité est d'authentifier l'identité des utilisateurs du réseau.

Protection : la sécurité des dispositifs est essentielle. Avec un système en réseau, tous les dispositifs peuvent être des points d'entrée pour une cyberattaque. Par conséquent, MasterCard a fait l'acquisition l'an dernier de NuData Security, une entreprise de technologie canadienne novatrice qui aide les entreprises à prévenir la fraude en ligne ou par téléphonie mobile. NuData renforce nos capacités, notamment en prévenant les cyberattaques ciblant les appareils des consommateurs, les prises de contrôle de comptes et les frictions en matière de renseignement.

Détection : on vise essentiellement à contrer une attaque avant qu'elle ne survienne. Nous investissons massivement dans l'intelligence artificielle, notamment avec l'acquisition récente de Brighterion, un chef de file mondial du secteur de l'IA, ce qui renforce notre capacité de détecter des attaques complexes. Les solutions d'IA de Brighterion aident MasterCard à trouver la fameuse aiguille dans une botte de foin lorsqu'on doit dépouiller d'énormes quantités de données.

Intervention : pour répondre efficacement aux menaces, l'échange d'information et la collaboration sont essentielles parmi les partenaires de l'industrie, les institutions financières et le FS-ISAC. Aux États-Unis, des équipes de préparation aux cyberurgences, ou CERTS, collaborent avec leurs homologues dans d'autres pays, dont le Canada.

Récupération : Comme d'autres chefs de file de l'industrie, MasterCard élabore et améliore sans cesse des plans de résilience pour s'assurer que nos plans de contingence fonctionnent, au besoin.

Ce plan inclut un moyen automatisé de machine en temps réel à une autre. C'est ce que nous faisons à un très haut niveau.

Please let me turn to our advice for governments which falls into five main areas.

First, in a networked interconnected digital world, we need cybersecurity solutions tailored to small- and medium-sized businesses. Cybercriminals will seek out the weak points in the system to launch an attack. Therefore, we need to provide a framework for small businesses to protect their operations. MasterCard is playing a leading role in defending small- and medium-sized businesses as we set up the Cyber Readiness Institute, which emphasizes the practical application of tools for small- and medium-sized businesses. The Institute also facilitates the workforce development needed to implement those cybersecurity management tools.

Second, companies frequently confront an expanding and overlapping set of cybersecurity regulations in different jurisdictions. Those need to be harmonized using a baseline framework. We understand good trilateral progress is being made here in the context of the NAFTA renegotiation, developing a common framework to align the management of cyber risk, which is encouraging.

Third, there is a need to improve identity management and authentication as more devices are connected online. We need a robust identity ecosystem to enable easier and more secure digital transactions, which safeguards the privacy of our cardholders.

Fourth, with the Internet of things, there will soon be 30 billion connected devices. This creates enormous opportunities for the digital economy, but it also increases the cyber risk. Therefore, governments and the private sector should develop standards to improve the interoperability and cyber-threat detection and prevention while removing friction from commerce.

Finally, as the cyber threat grows, governments and the private sector face a shortage of employees with cybersecurity skills. In fact, the world needs to start training the next generation of cyber experts, and government has a role to play. If you have kids or grandkids, get them hooked on cybersecurity. They can make a lot of money in their lifetime because right now the need is there, but the qualified cyber professionals are not.

I could talk for hours on this subject, but I only have seven minutes. I have provided today a snapshot of what we are doing and what we think governments should be doing. I must acknowledge that I know the Canadian government is working on a cybersecurity strategy. We took part in the consultation and look forward to its rollout. Unfortunately, we do not have the luxury of time when it comes to cyber-threats. Collaboration,

Permettez-moi maintenant de parler du conseil que nous avons donné aux gouvernements, qui porte sur cinq principaux secteurs.

Premièrement, dans un monde numérique en réseau interrelié, nous avons besoin de solutions en matière de cybersécurité adaptées aux petites et moyennes entreprises. Les cybercriminels trouveront les faiblesses dans le système pour lancer une attaque. Par conséquent, nous devons fournir un cadre pour permettre aux petites entreprises de protéger leurs opérations. MasterCard joue un rôle de chef de file pour défendre les petites et moyennes entreprises en mettant sur pied le Cyber Readiness Institute, qui met l'accent sur l'application pratique d'outils pour les petites et moyennes entreprises. L'institut favorise le perfectionnement de la main-d'œuvre nécessaire pour mettre en œuvre ces outils de gestion de la cybersécurité.

Deuxièmement, les entreprises doivent fréquemment gérer un ensemble croissant de règlements en matière de cybersécurité qui se chevauchent dans différentes instances. Il faut les harmoniser à l'aide d'un cadre de base. Nous sommes au courant des progrès trilatéraux qui sont accomplis dans le cadre de la renégociation de l'ALENA, où nous élaborons un cadre commun pour harmoniser la gestion des cyberrisques, ce qui est encourageant.

Troisièmement, il faut améliorer la gestion et l'authentification de l'identité à mesure que des appareils sont branchés en ligne. Nous avons besoin d'un écosystème d'identités solide pour assurer des opérations numériques plus sécuritaires, ce qui protège la vie privée des détenteurs de carte.

Quatrièmement, avec l'Internet des objets, on aura bientôt 30 milliards d'appareils connectés. Cela crée d'énormes occasions pour l'économie numérique, mais augmente aussi les risques cybernétiques. Par conséquent, les gouvernements et le secteur privé devraient élaborer des normes pour améliorer l'interopérabilité, la détection des cybermenaces et la prévention tout en éliminant les points irritants du commerce.

Enfin, à mesure que les cybermenaces s'intensifient, les gouvernements et le secteur privé sont confrontés à une pénurie d'employés qui possèdent des compétences en matière de cybersécurité. En fait, le monde doit commencer à former la prochaine génération d'experts en cybersécurité, et le gouvernement a un rôle à jouer. Si vous avez des enfants ou des petits-enfants, intéressez-les à la cybersécurité. Ils peuvent gagner beaucoup d'argent dans leur vie, car il y a un besoin maintenant, mais nous n'avons pas les professionnels qualifiés en matière de cybersécurité.

Je pourrais discuter du sujet pendant des heures, mais je n'ai que sept minutes. J'ai offert aujourd'hui un aperçu de ce que nous ferons et de ce que les gouvernements devraient faire, d'après nous. Je dois dire que je sais que le gouvernement canadien travaille à l'élaboration d'une stratégie en matière de cybersécurité. Nous avons participé aux consultations et attendons le déploiement avec impatience. Malheureusement,

information sharing, bringing all stakeholders to the table — all this is required to fight cybercrime. President Obama commissioned an expert task force on cybersecurity on which our CEO sat. That task force issued a series of recommendations. The CRI, which I mentioned earlier, is a direct offshoot of the task force emphasis on securing SMEs. I believe this is an issue so fundamental to the future of our economy and society that it needs attention and leadership at the highest levels.

MasterCard is ready to lend its expertise to the Government of Canada in much the same way.

Thank you to the committee for having me here, and I look forward to questions.

The Chair: Mr. Green, thank you very much. That was very helpful. We will now have questions from the senators.

Senator Stewart Olsen: Thank you very much for being here. It was very informative.

I admit I looked with skepticism on the government's announcement yesterday. I think there are massive difficulties they are going to have to overcome. For instance, this is a government where we couldn't manage a pay system, so I'm not sure how we will manage cybersecurity and provide information.

Your point, Mr. Green, on the talent pool is one I raised yesterday and it is a major concern. I would like to know what your advice would be. Where do you go to get trained? Who offers this? Should the government be putting more money into universities and community colleges, places that actually look at this and train people for this very important position?

Mr. Green: As part of the institute I mentioned, we have a number of different programs we're working on collaboratively with the federal government in the U.S., and that includes potentially creating internships where the cyberprofessionals have an opportunity to work for the government for a while and then have an opportunity to work for us.

We do a lot with universities in the U.S., just working with them to help establish the curriculum to train a cyberprofessional.

We also work with different organizations to allow people who are thinking about leaving the military to spend time with us, like in an apprenticeship program, to give them an

nous n'avons pas le luxe d'attendre en ce qui concerne les cybermenaces. La collaboration, l'échange de renseignements, la participation de tous les intervenants à la table sont nécessaires pour lutter contre le cybercrime. Le président Obama a mandaté un groupe d'experts sur la cybersécurité dont notre PDG a fait partie. Le groupe d'experts a formulé une série de recommandations. Le CRI, que j'ai mentionné plus tôt, est une ramification directe de l'accent que met le groupe d'experts sur la protection des PME. Je crois que c'est un problème fondamental pour l'avenir de notre économie et de notre société, car il faut y porter une attention et exercer un leadership à des niveaux plus élevés.

MasterCard est disposée à mettre à contribution son expertise pour le gouvernement du Canada à peu près de la même façon.

Je remercie le comité de m'avoir reçu aujourd'hui, et je vous remercie de vos questions.

Le président : Monsieur Green, merci beaucoup. C'était très utile. Nous allons maintenant passer aux questions des sénateurs.

La sénatrice Stewart Olsen : Merci beaucoup de votre présence ici. C'était très instructif.

J'admets que j'ai reçu avec scepticisme l'annonce que le gouvernement a faite hier. Je pense qu'il devra surmonter d'énormes difficultés. Par exemple, c'est un gouvernement qui n'a pas pu gérer un système de paie, alors je ne sais pas comment nous arriverons à gérer la cybersécurité et à fournir des renseignements.

Hier, j'ai soulevé le même point que vous, monsieur Green, concernant le bassin de talents. Il s'agit d'une source importante de préoccupations. Quels conseils auriez-vous à nous formuler? Où peut-on suivre la formation? Qui l'offre? Le gouvernement devrait-il investir davantage dans les universités et collèges communautaires, des établissements qui examinent la question et qui pourraient offrir aux gens la formation nécessaire à ce poste très important?

M. Green : Dans le cadre des activités de l'institut, dont j'ai parlé plus tôt, nous travaillons à divers programmes en collaboration avec le gouvernement américain, y compris la possibilité de créer des stages permettant aux cyberprofessionnels de travailler pendant un certain temps pour le gouvernement pour avoir ensuite la possibilité de travailler pour nous.

Nous travaillons beaucoup avec les universités américaines simplement pour les aider à créer le programme d'études nécessaire pour la formation d'un cyberprofessionnel.

Nous travaillons également avec diverses organisations pour permettre aux gens qui songent à quitter les forces armées, par exemple, de travailler pendant un certain temps avec nous, comme dans le cadre d'un programme d'apprentissage, pour leur

opportunity to see what it's like to work in the cyber field. There are many opportunities you guys could be working on.

Senator Stewart Olsen: Do you have any idea on what Canadian universities are doing?

Mr. Green: I'm sorry; I'm limited on what I know about Canadian universities.

Senator Tannas: Thank you for being here, gentlemen. I wanted to get Mr. Smith's comments and then anybody else who wants to chip in with respect to the amount of money invested in bringing to justice the people who are perpetrating crimes today.

We've heard testimony in different ways where we know there are billions of dollars being taken from people, and that's based on what is reported and an understanding this is the tip of the iceberg. Most people are too embarrassed to report it, or it's too small, or it's so large and embarrassing they won't report it.

It seems to me it should be easier to hunt these people down, so I'm led to believe there is not an adequate effort going on. I know the government pledged \$116 million over five years, so \$24 million a year — probably on a head count basis, 250 more officers on an annual basis out there hunting down. Is that enough? Are we actually doing enough? I get that we're doing enough to protect our macro situation, and that's national security stuff, but are we doing enough to track down the petty thieves, the guys who buy for .1 BTC their own little criminal enterprise, and is \$24 million a year going to get that job done?

Mr. Smith: I would start by saying, no, it's probably not enough and it never will be enough. The biggest challenge for law enforcement in tracking down and dealing with cyber criminals is in order to find them, you have to think like a criminal. And I don't think we teach people to think like criminals. So they have a big task in front of them.

I think the most important thing for the business community and for individuals is to be able to protect themselves to a certain degree and make themselves less of a target. The reality for most of the petty cyber crimes, under \$5,000 in terms of ransomware, for instance, those are not particularly sophisticated actors, and it's not particularly sophisticated software. It's relatively easy to deal with if you have the awareness not to click on it in the first place and, if you do, if you have the right systems in place to be able to bring your systems back up to speed quickly. It's about resilience. To go back to your original question, is it sufficient to go after all the petty criminals out there, no, it's not, but there are probably more important things to deal with in terms of critical infrastructure, for instance. You want to go after that first.

permettre d'avoir une idée du travail dans le secteur de la cybersécurité. Il y a de nombreuses options qui s'offrent à vous.

La sénatrice Stewart Olsen : Avez-vous une idée de ce que font les universités canadiennes?

M. Green : Je suis désolé, mais mes connaissances concernant les universités canadiennes sont limitées.

Le sénateur Tannas : Messieurs, merci d'avoir accepté notre invitation. J'aimerais d'abord obtenir les commentaires de M. Smith, et les autres témoins pourront intervenir par la suite, s'ils le souhaitent, sur les sommes investies pour poursuivre en justice ceux qui commettent ces crimes.

Selon les témoignages que nous avons entendus, ces crimes totalisent des milliards de dollars, et ce ne sont que les crimes qui sont rapportés sachant que ce n'est que la pointe de l'iceberg. La plupart des gens ont trop honte pour signaler ces crimes, ou les sommes volées sont trop petites ou trop importantes, ce qui constitue une autre source de honte.

À mon avis, il devrait être plus facile de traquer ces gens, ce qui me porte à croire que l'effort est insuffisant. Je sais que le gouvernement a promis d'investir 116 millions de dollars au cours des cinq prochaines années, soit 24 millions de dollars par année — probablement en fonction de l'effectif, 250 agents de plus, par année, pour traquer ces criminels. Est-ce suffisant? L'effort est-il suffisant? Je comprends que nous déployons suffisamment d'effort au sens large et qu'il s'agit d'une question de sécurité nationale, mais déployons-nous suffisamment d'effort pour traquer les petits voleurs, ceux qui s'achètent une petite entreprise criminelle avec 0,1 bitcoin? Est-ce que 24 millions de dollars par année, c'est suffisant?

M. Smith : Je dirais d'abord que, non, ce n'est probablement pas suffisant et ce ne le sera jamais. Le plus gros défi pour les autorités policières, c'est que pour traquer et trouver ces cybercriminels, il faut penser comme un criminel. À ma connaissance, on n'enseigne pas aux gens à penser comme des criminels. C'est donc une tâche importante qui les attend.

À mon avis, le plus important pour la communauté des affaires et les particuliers, c'est de se protéger eux-mêmes, dans une certaine mesure, et de prendre les mesures nécessaires pour ne pas devenir une cible. La réalité, c'est que la plupart des individus qui commettent ces petits cybercrimes, par exemple, les rançongiciels de moins de 5 000 \$, ne sont pas vraiment sophistiqués et les logiciels qu'ils utilisent ne le sont pas non plus. Ils sont relativement faciles à bloquer si l'on sait qu'il ne faut pas cliquer sur les courriels en question et si l'on a en place un système de réserve adéquat pour récupérer ses informations, si jamais on clique sur le courriel. C'est une question de résilience. Pour revenir à votre question, est-ce suffisant pour traquer tous les petits criminels? Non, mais il est probablement plus important de s'attaquer aux problèmes liés à l'infrastructure critique, par exemple. C'est la première chose qu'il faut régler.

Senator Tannas: I'm always frustrated with the "either-or." Why can't have an "and," where we do both? I think back to New York City and Mayor Giuliani who went after both the mafia and the guy who spit on the street, and that's how New York went from being a hole to being a wonderful place we all like to go to. I remember when it was the opposite. Is there not something we're missing here? Don't petty criminals start out as petty criminals and become something larger?

Mr. Smith: I think what you're chasing is the larger crimes.

In other words, if you follow the money, there are larger criminal enterprises behind those petty criminals, so that's what we should be going after.

To your point, is \$24 million or 250 new officers enough to deal with that? Probably not. But we do need to work more closely with other law enforcement agencies around the world. This is not a Canadian problem; this is a global problem.

Mr. Green: I was recently at the FBI CISO Academy. Just like serial killers, hackers actually have a background or past, so you can have a behavioural analyst analyze the hacker and see what their tendencies are.

I think the problem, as far as enforcement goes, is you just don't have enough officers who are trained. It's completely different and new, so a lot of training is required to bring them up to speed. Then you have hackers who work — it's an international crime. Even for the small things, you can have international boundaries you have to overcome. Partnering with other countries, especially those where it may be more difficult to get at the bad guys, those are things that, for petty crimes, your local officers would have to contend with.

The Chair: Senator Dagenais, before you start, let's make sure we have our earphones in place and we're ready to go with translation.

Senator Dagenais: I speak English, but I prefer in French.

[Translation]

My first question is for Mr. Green. Often, with cases of attempted credit card fraud, consumers may have to limit their card use for a certain period of time. Though this decision may bother consumers, it is indeed necessary. For their well-being, can you tell us, Mr. Green, at what point does attempted credit card fraud become a cyber attack? Do you have a policy that aims to inform potential victims of a cyber attack? We know that many people — myself included — fall victim to attempted credit card fraud, without it being a cyber attack. However, there must be a moment when you realize that you are not dealing with

Le sénateur Tannas : Je suis toujours frustré d'entendre que c'est soit l'un, soit l'autre. Pourquoi ne pourrait-on pas faire les deux? Je me souviens du maire Giuliani, à New York, qui s'est attaqué à la fois à la mafia et à Monsieur Tout-le-monde qui crache dans la rue. C'est ainsi que New York est passée d'un trou à un endroit merveilleux que nous aimons tous visiter. Je me souviens de l'époque où c'était le contraire. Est-ce qu'on ne manque pas le bateau? Les petits criminels ne deviennent-ils pas de grands criminels?

M. Smith : Je crois qu'il faut traquer les crimes plus importants.

Autrement dit, si vous suivez l'argent, vous verrez qu'il y a de grandes entreprises criminelles derrière ces petits crimes. Il faudrait s'attaquer à ces entreprises.

Pour revenir à votre question, à savoir si 24 millions de dollars ou 250 nouveaux agents est suffisant, je dirais probablement que non. Toutefois, nous devons travailler plus étroitement avec les autres autorités policières du monde. Ce n'est pas un problème canadien; c'est un problème mondial.

M. Green : J'ai visité récemment la FBI CISO Academy. Tout comme les tueurs en série, les pirates informatiques ont un passé. Un analyste en comportement peut donc analyser le pirate informatique et déceler ses tendances.

À mon avis, le problème en ce qui a trait à l'application, c'est le manque d'agents formés. Il s'agit de quelque chose de totalement différent et de nouveau. Il faut donc beaucoup de formation pour être à jour. Ensuite, il y a le pirate informatique qui travaille — il s'agit d'un crime international. Même pour les petits crimes, il faut franchir des frontières internationales. Il peut donc être difficile pour les agents locaux qui enquêtent sur de petits crimes d'établir des partenariats avec d'autres pays, surtout les pays où il est plus difficile de trouver les méchants.

Le président : Sénateur Dagenais, avant d'amorcer votre intervention, assurons-nous que les écouteurs fonctionnent et que l'interprétation est prête.

Le sénateur Dagenais : Je parle anglais, mais je préfère m'exprimer en français.

[Français]

Ma première question s'adresse à M. Green. Souvent, lorsqu'il y a eu tentative de fraude avec une carte de crédit, il est possible que l'on doive réduire l'utilisation de la carte pendant une certaine période de temps. Évidemment, cette intervention, qui peut s'avérer dérangeante pour le consommateur, est tout de même nécessaire. Monsieur Green, pour le bien des consommateurs, pouvez-vous nous dire à quel moment une tentative de fraude à l'aide d'une carte de crédit devient une cyberattaque? Avez-vous une politique qui vise à informer les victimes potentielles d'une cyberattaque? On sait que plusieurs

mere attempted fraud, but with a cyber attack, at which point you must inform your clients.

[English]

Mr. Green: There are a couple of things I think about here. One, when it's fraud, we will notify or provide solutions to help the issuer identify the potential fraud on the card — and that's what people most commonly encounter. When there's a larger breach, when we identify a point of compromise that's been attacked, we don't do the notification. The victim is the organization that must do the notification. The victim is the one required to notify the impacted customers that they have been breached, they have been compromised, and because of that, those cards are at risk.

So we don't do the notification. We help in the identification at the point of compromise, but it's on the victim to do that notification.

[Translation]

Senator Dagenais: Mr. Gordon, can you give us examples of cybersecurity products, and tell us if small companies with more modest budgets can afford them?

[English]

Mr. Gordon: Yes. Eventually the products will be. We are developing some specific products for small companies that don't have the large IT infrastructure, so very tailored to their needs: Here's something very practical for them to be able to do, and they will use them. It will actually work nicely with some of the efforts that Mr. Smith was talking about relative to the Cyber Essentials program. I see those two going hand in hand in terms of here are the regulations and guidance, on one side; and at the same time, here's some practical advice, something you can do for a small company that, as I say, doesn't have the big IT shop or the expertise to go through it. So, yes, we're developing that, and we're starting to get small companies joining us now.

Senator Wetston: I think Senator Tannas pursued this issue yesterday. I may be incorrect, but I think the issue we were talking about was financial market institutions yesterday and hearing from witnesses. I think it was yourself, Senator Tannas, who pursued the potential attacks on other infrastructure — hydroelectric facilities, nuclear facilities, telecommunication. Was that you or am I inappropriately pointing you out here?

personnes — moi y compris — sont victimes d'une tentative de fraude sur leur carte de crédit, sans que ce soit une cyberattaque. Cependant, il doit y avoir un moment où vous vous rendez compte qu'il ne s'agit pas seulement d'une tentative de fraude, mais bien d'une cyberattaque, et que vous devez informer vos clients.

[Traduction]

M. Green : Quelques points me viennent à l'esprit. D'abord, lorsqu'il s'agit d'une fraude, nous informons l'émetteur ou lui offrons des solutions pour l'aider à identifier la fraude potentielle sur la carte — c'est la situation que la plupart des gens vivent. Lorsqu'il s'agit d'une infraction plus importante, que nous identifions le point de compromission attaqué, nous ne communiquons pas avec les consommateurs. C'est l'organisation la victime, et c'est donc à elle que revient la responsabilité de communiquer avec les clients. C'est elle qui doit communiquer avec ses clients pour les informer qu'ils ont été victimes de cette infraction et que leur information a été compromise et que, pour cette raison, leur carte est à risque.

Nous ne nous chargeons pas de cette communication. Nous aidons à identifier le point de compromission, mais il revient à la victime de communiquer avec ses clients.

[Français]

Le sénateur Dagenais : Monsieur Gordon, pouvez-vous nous donner des exemples de produits de cybersécurité et nous dire s'ils sont à la portée des petites entreprises dont les budgets pour se les procurer sont moins vastes?

[Traduction]

M. Gordon : Oui. Ils finiront par l'être. Nous travaillons à l'élaboration de certains produits bien précis pour les petites entreprises qui ne disposent pas d'une importante infrastructure de TI. Ce sont des produits qui répondent à leurs besoins. Si nous leur offrons des produits qui pourraient leur être pratiques, ils les utiliseront. Cela ira bien avec certains des efforts déployés par M. Smith relativement au programme Cyber Essentials. Je crois que les deux iront de pair en matière de réglementation et d'orientation, d'un côté, et de l'autre côté, pour la formulation de conseils pratiques pour aider les petites entreprises qui, comme je l'ai dit, ne disposent pas d'une importante infrastructure de TI ou de l'expertise nécessaire. Donc, oui, nous travaillons à l'élaboration de ce genre d'outils et de petites entreprises commencent à se joindre à nous.

Le sénateur Wetston : Je pense que le sénateur Tannas a abordé la question hier. Je fais peut-être erreur, mais je pense qu'hier, nous traitions des institutions des marchés financiers et entendions des témoins. Il me semble que c'est vous, sénateur Tannas, qui avez évoqué les attaques potentielles contre d'autres infrastructures, comme les installations hydroélectriques et

Senator Tannas: You are.

Senator Wetston: If it was, it was a great question.

I want to follow that up with you. There are a couple of other questions within this.

For example, Mr. Green, where do you fit into the payment structure? Do you have any regulatory oversight in Canada or the U.S. with respect to the payment system? That's a second question that you might think about before I get to this first one.

What are your collective thoughts around cybersecurity and cyber attacks with respect to the infrastructure beyond financial institutions?

Mr. Gordon: I think it's critical that we look at this holistically. It's one of the reasons why the CCTX was structured the way it was, by bringing all companies together. Because the same kind of attack that will go after a hospital or university is the same kind of attack that will go after a small business or the financial institution. So it's critical we have all those sectors working together, because the attackers are not distinguishing between a financial institution or another type of business.

The second thing is they're using the supply chain to access into a variety of companies. They will go after the weakest link. It may be the small company that provides services into multiple other kinds of sectors. It's imperative we look at this holistically. Attackers are just looking for an easy door, and then they will go inside the system. We've got to be protecting all of them.

Mr. Smith: The other side of the equation is the critical infrastructure you're talking about: the hospitals, hydroelectric and nuclear facilities, your street infrastructure, your stoplights, what have you. All of that will impact the cost of doing business. In other words, you want to make sure you have a competitive environment to work in; and if you can't turn the lights on and if you don't have access to good water, suddenly it's no longer a good place to do business, and that affects everybody.

Senator Wetston: The relationship between the need to have cyber resilience, but also to be able to operate your business, is obviously important.

Mr. Green, I asked you a question about how you fit into the payment system, and maybe you don't. But perhaps you also have a comment with respect to running your business and spending hundreds of millions of dollars, I'm sure, on

nucléaires et les infrastructures de télécommunication. Était-ce vous, ou est-ce que je me trompe?

Le sénateur Tannas : Vous vous trompez.

Le sénateur Wetston : Si c'était vous, c'était une excellente question.

Je veux continuer sur la question avec vous, car le sujet soulève d'autres interrogations.

Par exemple, monsieur Green, quel rôle jouez-vous au sein de la structure de paiement? Faites-vous l'objet d'une surveillance de la part d'un organisme de réglementation au chapitre du système de paiement au Canada ou aux États-Unis? Voilà une deuxième question à laquelle vous pourriez réfléchir avant que j'en arrive à la première.

Collectivement, que pensez-vous de la cybersécurité et des cyberattaques relatives aux infrastructures au-delà des institutions?

M. Gordon : Je pense qu'il est essentiel que nous examinions la situation d'un point de vue holistique. C'est une des raisons pour lesquelles l'Échange canadien de menaces cybernétiques est structuré comme il l'est, en réunissant toutes les entreprises, car l'attaque qui visera un hôpital ou une université s'apparentera à celle qui ciblera une petite entreprise ou une institution financière. Il faut donc absolument que tous les secteurs travaillent ensemble, car les attaquants ne font aucune distinction entre une institution financière ou un autre genre d'entreprise.

Sachez en outre que les attaquants exploitent la chaîne d'approvisionnement pour s'en prendre à diverses entreprises, s'attaquant au maillon faible, comme la petite entreprise qui fournit des services à une multitude de secteurs. Nous devons impérativement adopter une approche holistique. Les attaquants sont à l'affût d'une porte facile à forcer, puis ils s'infiltreront dans le système. Nous devons protéger toutes les entreprises.

M. Smith : De l'autre côté de l'équation, il y a les infrastructures essentielles que vous évoquez : les hôpitaux, les installations hydroélectriques et nucléaires, les infrastructures routières, les feux de circulation et j'en passe. Tout cela aura une incidence sur les coûts d'affaires. Autrement dit, il faut s'assurer de pouvoir travailler dans un environnement concurrentiel, et si on ne peut pas allumer les lumières ou avoir accès à de l'eau de qualité, le milieu de travail s'en trouve subitement affecté et tout le monde est touché.

Le sénateur Wetston : Le lien entre la nécessité d'assurer la cyberrésilience et le besoin de pouvoir exploiter son entreprise est de toute évidence important.

Monsieur Green, je vous ai interrogé sur votre rôle dans le système de paiement, mais peut-être n'en avez-vous pas. Mais pouvez-vous nous parler du fonctionnement de votre entreprise, où vous devez sûrement investir des centaines de millions de

cybersecurity or safety and security of the system. Maybe that's an excessive amount, but I'm sure it's quite considerable. Any thoughts about that?

Mr. Green: When it comes to the spend for security, I've not been in a situation where I've not been able to get new capabilities we thought were important for MasterCard. We spend lots, and we will continue to spend more. It's something our CEO has been very clear and dedicated with us about.

Our CEO actually had a similar question of me, making sure we were connected to those interdependent sectors like power and telecommunications, so making sure we have close ties. If we are up and available, but our customers can't connect or talk to one another, or they don't have power for their businesses, that will impact our ability to do the right thing for the customers.

The other question you asked was whether we are regulated, and do we have bodies that come in and oversee us? We do. Annually, we have the FFIEC, Federal Financial Institutions Examination Council. They evaluate what it is we're doing for MasterCard. We have other countries that do similar things. That's where the harmonization of regulatory requirements would be greatly helpful to us.

While compliance is not security, to me — so understanding we meet the compliance requirements, those are things we have to do. If there are 25 different ways of doing it, I spend my time meeting the compliance requirement, and then improving the security of the organization.

Senator Wetston: I have a number of questions here. I would like to try, if I could — and perhaps we'll have a second round.

As we're thinking about this as a report and being able to usefully contribute to public knowledge, and also to provide advice to government as they're continuing to develop rules, regulations and requirements around cybersecurity, I remember hearing a TED Talk once where this physicist said the following, "If you're an algorithm, you have a good future." That's almost what you were getting at when it comes to being able to educate yourself or work in the cybersecurity space.

But if you think about cybersecurity and about the ecosystem, the broader ecosystem, which I would describe as artificial intelligence, big data, interconnectedness — and that's my second question: I'll get to that in a moment — where do you see cybersecurity in the ecosystem, of all of these things continuing to transform our economy: Canada, U.S. and globally? I'd like to hear from all of you, if you have a comment.

dollars pour assurer la cybersécurité et la sécurité des systèmes? Ce chiffre est peut-être excessif, mais je suis certain que la somme est substantielle. Avez-vous des observations à formuler à ce sujet?

M. Green : Quand vient le temps d'investir dans la sécurité, il ne m'est jamais arrivé de ne pas pouvoir acquérir de nouvelles capacités que nous jugions importantes pour MasterCard. Nous dépensons beaucoup et nous continuerons de dépenser davantage. Notre directeur général s'est montré très sérieux et on ne peut plus clair à ce sujet.

En fait, il m'a posé une question semblable pour s'assurer que nous entretenons des liens étroits avec les secteurs indépendants, comme ceux de l'électricité et des télécommunications. Si nous sommes à la disposition des clients, mais que ces derniers ne peuvent se connecter, parler entre eux ou alimenter leur entreprise en électricité, il nous sera difficile de faire ce qu'il faut pour eux.

Vous nous avez également demandé si nous sommes réglementés et si des organes nous supervisent. La réponse est oui. Chaque année, le Federal Financial Institutions Examination Council évalue ce que nous faisons pour MasterCard. D'autres pays font la même chose. Voilà où l'harmonisation des exigences réglementaires nous aide beaucoup.

Même si conformité n'est pas synonyme de sécurité, nous devons comprendre que nous satisfaisons aux exigences; ce sont les choses que nous devons faire. S'il existe 25 manières de procéder, je passerai mon temps à chercher à satisfaire aux exigences, puis à améliorer la sécurité de l'organisation.

Le sénateur Wetston : J'ai un certain nombre de questions. Je voudrais essayer de les poser, si possible, et nous tiendrons peut-être un deuxième tour.

Alors que nous réfléchissons à notre rapport et à la manière dont nous pourrions contribuer utilement à informer le public et prodiguer des conseils au gouvernement, qui continue d'élaborer des règles, des règlements et des exigences au sujet de la cybersécurité, je me souviens d'avoir entendu, au cours d'une conférence TED, un physicien qui affirmait que si on est un algorithme, on est promis à un bel avenir. Cela revient presque à ce que vous dites sur le fait qu'il faut pouvoir s'éduquer ou travailler dans le domaine de la sécurité.

Cependant, si on pense à la cybersécurité et à l'écosystème dans son ensemble, lequel comprend l'intelligence artificielle, les mégadonnées et l'interconnexion — sur lesquelles portera ma deuxième question et auxquelles j'arriverai dans un instant —, que pensez-vous de la cybersécurité dans cet écosystème et de toutes ces choses qui continuent de transformer l'économie au Canada, aux États-Unis et dans le monde? J'aimerais entendre chacun d'entre vous si vous avez un commentaire à formuler.

Mr. Smith: One of the things I think we should probably have a larger conversation about is the Internet of things, or the Internet of everything, as some companies have characterized it, where you have billions of devices being deployed — some of them in the homes, some of them artificial intelligence, or at least machine learning — that are not necessarily designed with security in mind. I think that's one of the bigger challenges we're going to see in the next 10 years. As the evolution and the deployment and the ubiquity of these devices becomes much more common, there's going to be a lot more in the way of paths in the door. So anything connected to those devices suddenly becomes a risk, and I think we need to start thinking about risk a lot more carefully.

Mr. Green: Cybersecurity should be like the air you breathe, as a part of anything you do. The technology we deploy, we come up with, is all meant to make things easier for humans. But as we make things easier for humans, as Scott said, oftentimes we're deploying things without thinking about the security implications of what it is we've deployed. It has to be part of what we're thinking all the time when we create these new things, because there is someone out there, once they get a hold of it, who will find a weakness if you haven't found it.

Mr. Gordon: The other part about cybersecurity is it's an economic opportunity. As you were saying, senator, we're looking at big data and that sort of thing, and the processing of it. Data has now become the new currency; and if you can go to an environment where you can do that in a secure way, that's a competitive advantage over areas that you can't do that.

I think in Canada we're well positioned. We have a lot of talented start-up companies that have a high level of expertise in the cybersecurity area. We have the talent pool. We have the legislative underpinning for the protection of privacy. We understand all that. So we have a great opportunity here. Yes, we have to do it to protect our business, but it's also a business opportunity for the country as a whole.

Senator Tkachuk: Just a couple of questions on access. I've had a number of experiences with credit card fraud. In other words, one time some guy — it was a 7-Eleven or something — had taken out 10 bucks or 20 bucks at a time. I got a call from Visa. The other time was more serious; it was about 3,600 bucks. Because I go on the Internet to check my credit cards almost every second day, I found it right away, but it was done through a Facebook account.

How are these credit cards — are they sold by an employee in the business who is making money selling the credit card information from a merchant I used, or is it the result of some

M. Smith : Selon moi, il faudrait probablement tenir une discussion élargie sur l'Internet des objets ou de tout, pour reprendre l'appellation qu'utilisent certaines entreprises pour parler des milliards d'appareils déployés qui n'ont pas été nécessairement conçus avec la sécurité en tête, comme la domotique, l'intelligence artificielle ou, au moins, l'apprentissage machine. Je pense que c'est là un des défis les plus importants que nous aurons à relever au cours des 10 prochaines années. À mesure que l'évolution, le déploiement et l'ubiquité deviennent de plus en plus courants, les manières de pénétrer les systèmes se multiplieront. Tout ce qui est connecté à ces appareils pose tout à coup un risque, et je pense que nous devons commencer à réfléchir un peu plus attentivement au risque.

M. Green : La cybersécurité devrait, à l'instar de l'air qu'on respire, faire partie de tout ce que l'on fait. Les technologies que nous inventons et déployons visent à faciliter la vie des êtres humains. Cependant, comme Scott l'a souligné, nous déployons souvent des dispositifs sans penser à leurs conséquences sur la sécurité. Nous devons toujours avoir cette dernière à l'esprit quand nous concevons de nouveaux appareils, car quelqu'un s'en emparera et en décèlera les faiblesses si nous ne les avons pas détectées.

M. Gordon : La cybersécurité offre également une occasion économique. Comme vous l'avez indiqué, sénateur, nous nous intéressons aux mégadonnées et à leur traitement. Les données sont maintenant devenues la nouvelle devise, et quiconque bénéficie d'un environnement permettant de les gérer en toute sécurité dispose d'un avantage concurrentiel sur ceux pour qui ce n'est pas le cas.

Je pense que le Canada fait bonne figure à cet égard, puisqu'il peut compter sur de nombreuses nouvelles entreprises talentueuses dotées d'une solide expertise dans le domaine de la cybersécurité. Nous avons le bassin de talent et les fondements législatifs permettant de protéger la vie privée. Nous comprenons tout cela. Nous bénéficions donc d'une occasion formidable. Oui, nous devons agir pour protéger notre entreprise, mais la cybersécurité représente aussi une occasion d'affaires pour l'ensemble du pays.

Le sénateur Tkachuk : Je n'ai que quelques questions sur l'accès. J'ai été victime d'un certain nombre de fraudes par cartes de crédit, notamment de la part d'un homme qui effectuait des achats de 10 ou 20 \$ dans un 7-Eleven ou un commerce quelconque. J'ai reçu un appel de Visa. L'autre fraude, plus grave, s'élevait à quelque 3 600 \$. Comme je consulte mes cartes de crédit sur Internet presque aux deux jours, je m'en suis rendu compte immédiatement, mais le fraudeur passait par l'entremise d'un compte Facebook.

Comment ces cartes de crédit... Sont-elles vendues par un employé de l'entreprise qui se fait de l'argent en refilant l'information obtenue d'un commerce où je me suis rendu, ou

cyber attack on a larger scale I was unaware of? Where are most of them done? How are most of them done?

Mr. Green: Large-scale breaches are how a lot of it gets into the fraud ecosystem, where they breach a major merchant or processor, capture the card information, and then break it up and sell it on the dark web. But a lot of it has been, over time, captured through skimmers. There are different methods attackers or bad guys have used to collect information.

If you think about the improvements in the technology, like going to EMV, which discourages the capture of the magnetic stripe, and the things we're doing with new data, these will create newer ways to secure the information used in the transaction to limit the availability of those things that can be commoditized and sold on the dark web.

Senator Tkachuk: Are you tough with people who do — in other words, in one case a merchant was giving out cash on a credit card or a credit card number. I'm not sure how that transaction took place. He obviously didn't have my credit card. I had my credit card. So he either had my number or he had information on it.

Is the merchant punished? How does that work? Obviously there's some complicity here; they work together, the employee and the guy he was giving the cash to.

Mr. Green: If they're complicit, that's a criminal offence, and we will work with the enforcement agencies and the issuing banks to do the right thing, if they were actually a part of the scheme. Mostly they're not. Mostly it's use of fraudulent means to present the credit card credential to try to obtain service or goods.

Senator Tkachuk: Do they duplicate? Is the card actually duplicated? In other words, is there a fake card with a number on it that they run through a machine, or does the guy just give them numbers and the guy gives them cash? How does that work?

Mr. Green: There are a lot of counterfeit cards. That's why moving to EMV and to digital payments over mobile devices provides a new opportunity to reduce the availability of using the counterfeit card. So, yes, counterfeit cards are what they take into stores to actually commit their crimes.

Senator Tkachuk: I'm going to ask a couple of questions on emails, because that's the way the bad stuff gets into your computer.

est-ce à cause d'une cyberattaque de grande envergure dont je n'ai pas entendu parler? À quel endroit la plupart de ces fraudes sont-elles commises? De quelle façon sont-elles commises?

M. Green : Une grande partie des données se retrouvent dans l'écosystème de fraude à la suite d'atteintes majeures, c'est-à-dire lorsqu'on porte atteinte à la cybersécurité d'un grand commerçant ou d'un processeur, qu'on saisit l'information de la carte, qu'on la fractionne et qu'on la vend sur le Web invisible. Mais au fil du temps, les copieurs de carte se sont emparés de nombreuses données. Les cybercriminels ou les malfaiteurs ont utilisé différentes méthodes pour recueillir l'information.

Si on pense aux améliorations technologiques, comme la technologie EMV, qui décourage la saisie de la bande magnétique, et à ce que nous faisons avec les nouvelles données, on comprend que cela permet de créer de nouvelles façons de protéger l'information utilisée dans une transaction pour limiter l'accès aux données qui peuvent être marchandisées et vendues sur le Web invisible.

Le sénateur Tkachuk : Vous montrez-vous durs envers... Autrement dit, à titre d'exemple, un marchand donnait de l'argent au moyen d'une carte de crédit ou d'un numéro de carte de crédit. Je ne sais pas comment la transaction s'est faite. De toute évidence, il n'avait pas ma carte de crédit. C'est moi qui l'avais. Par conséquent, soit qu'il en avait le numéro, soit qu'il avait l'information sur la carte.

Le marchand est-il puni? Comment procède-t-on? C'est manifestement un complice; l'employé et la personne à qui il a remis l'argent travaillent ensemble.

M. Green : S'ils sont complices, c'est alors un acte criminel, et nous travaillerons avec les organismes d'application de la loi et les banques émettrices pour faire la bonne chose, s'ils ont pris part au stratagème. Ce n'est généralement pas le cas. Cela consiste surtout à recourir à des moyens frauduleux pour présenter les renseignements de la carte de crédit dans le but d'obtenir un service ou des biens.

Le sénateur Tkachuk : Sont-elles reproduites? La carte est-elle reproduite? Autrement dit, est-ce une fausse carte avec un numéro qui est insérée dans une machine, ou la personne se contente-t-elle de donner les chiffres en échange d'argent? Comment procède-t-on?

M. Green : Il y a beaucoup de cartes contrefaites. C'est la raison pour laquelle le recours à la technologie EMV et aux paiements numériques à l'aide d'appareils mobiles offre un nouveau moyen de réduire l'utilisation de cartes contrefaites. Donc, oui, les malfaiteurs se servent de cartes contrefaites dans les commerces pour commettre leur crime.

Le sénateur Tkachuk : Je vais poser quelques questions sur les courriels, car c'est ainsi que le contenu malveillant entre dans l'ordinateur.

I think a lot of people do the same thing I do. I delete everything I don't absolutely recognize, which means I miss a lot of information I should get because I delete it, and only because I'm afraid of what may happen.

How do we get past that? Do we return to the fax machine to ensure security? There has to be a way. This is becoming more and more prevalent, and I don't know if there's a way to stop it. I know what you're all trying to do and everything else, but the criminal mind is a genius mind and they find ways to do it. If it's infecting computers, they're stealing information, they're blackmailing you, getting your bank records, private pictures you may have, all of that stuff becomes public. Help me out here.

Mr. Smith: My first comment is I would like you to manage my inbox for me, because I'm not good at deleting things.

My second comment is all of the emails you're getting where there is malicious software, there's always going to be that link. If you hover over the link, you will see what the URL is, and you will know that URL is not something you want to go anywhere near. It's usually pretty obvious. So that's an awareness thing.

We have to be careful not to conflate what happens to individuals with what's happening to businesses, because they're somewhat separate. Once a business is compromised, it can be a lot more devastating to that business because it's also going to affect all their employees.

The other thing we have to remember is many of the security breaches within a business happen because of something internally. Either somebody has clicked the wrong thing or it's malicious internally. So there needs to be some kind of awareness amongst employers and we need to find tools to combat that.

Your point about the emails and what they look like, they're getting a lot more sophisticated. Internally, it looks like it's coming from either your CEO or your finance department, asking you to sign off on something. So it's not even software anymore; it's something where they're actually collecting money for something.

Mr. Green: Seventy per cent of the major breaches you see hitting the headlines are the result of a phishing attack or a spear phishing attack, just like you described. So we have layers of controls to manage and control the email, but still some will get through. There's a dependency on the employee to do the right thing.

We make sure they clearly say the security of MasterCard isn't just on the security team. Every individual in this company is responsible for security of MasterCard.

Je pense que beaucoup de personnes font la même chose. Je supprime tout ce que je ne reconnais pas tout à fait, ce qui signifie que je supprime beaucoup d'information que je devrais recevoir, et seulement parce que j'ai peur de ce qui peut arriver.

Comment pouvons-nous surmonter le problème? Devrions-nous utiliser de nouveau des télécopieurs pour nous protéger? Il doit y avoir un moyen. Cela devient de plus en plus courant, et j'ignore s'il y a un moyen d'y mettre fin. Je sais ce que vous essayez tous de faire et tout le reste, mais les criminels font preuve de génie et trouvent des moyens d'arriver à leurs fins. S'ils veulent infecter des ordinateurs, ils volent de l'information, ils font du chantage, ils obtiennent des dossiers bancaires — et des photos intimes s'il y en a — et tous ces renseignements deviennent publics. Aidez-moi à comprendre.

M. Smith : Je vais d'abord dire que j'aimerais que vous gériez ma boîte de réception, car la suppression de messages n'est pas mon fort.

Je tiens ensuite à mentionner que dans tous les courriels que nous recevons qui contiennent des logiciels malveillants, il y a toujours un lien. Lorsque vous le survolez, vous voyez l'adresse URL, et vous savez que vous voulez vous tenir loin. C'est habituellement évident. C'est une question de sensibilisation.

Nous devons faire attention de ne pas confondre la situation des particuliers avec celle des entreprises, car ce n'est pas tout à fait la même chose. Une fois qu'une entreprise est menacée, les conséquences peuvent être beaucoup plus graves étant donné que tous ses employés seront touchés.

L'autre chose qu'il ne faut pas oublier, c'est qu'une grande partie des atteintes à la sécurité dans une entreprise se produisent à cause de circonstances à l'interne. Soit que quelqu'un a cliqué sur la mauvaise chose, soit que le malfaiteur est sur place. Il doit donc y avoir une sorte de sensibilisation des employés, et nous devons trouver les outils pour nous attaquer au problème.

À propos de ce que vous avez dit concernant les courriels et leur apparence, ils sont de plus en plus subtils. Dans une entreprise, on peut croire qu'ils viennent du PDG ou du service des finances, qui vous demande de signer quelque chose. Donc, ce n'est même plus des logiciels; cela consiste plutôt à demander de l'argent pour quelque chose.

M. Green : Soixante-dix pour cent des atteintes majeures à la sécurité qui font les manchettes sont le résultat d'une attaque par hameçonnage ou par hameçonnage ciblé, comme vous l'avez décrit. Nous avons donc des niveaux de contrôles à gérer ainsi que les courriels, mais certains malfaiteurs réussissent quand même à se faufiler. Nous dépendons des employés qui doivent faire la bonne chose.

Nous veillons à ce que les employés sachent que la protection de MasterCard ne dépend pas seulement de l'équipe de sécurité. Tous les employés sont responsables de protéger l'entreprise.

In addition, we've recently enabled progressive disciplinary action for those individuals who repeatedly click or infect machines in our environment, subject to termination. So three strikes, you're out.

The Chair: I have a couple of quick questions before we go to second round, if I may. I'm interested if any of you gentlemen can identify a country you think is best practice in managing these issues now.

Mr. Gordon: There are a variety of ways to look at that. Certainly some countries have invested significantly as a country in developing some technologies. Israel would be a good example, from incubating small companies coming up in the cyber sector. The United States, on the standards side of things, is leading the world. The National Institute for Standards is putting excellent products out and good guidance. Canada actually adopts a lot of those same practices. The United Kingdom is doing some interesting work with blending together what's provided for by the government on some of the standards of work for small- and medium-sized companies. It's a blending of those. Pick the best from several of those countries. I think those three are very good.

Mr. Green: The countries Robert described are things that I think about. I think most helpful to me as a protector of an organization are those areas of collaboration between the government and the industry. So I do think within the U.S. the partnership, through things like the FS-ISAC or where government is a heavy player, we, as different companies, bring a lot to the table. It allows us to do things like sending leadership from my team into another company. Canadian Tire is actually a member of the FS-ISAC. We send our leaders into Canadian Tire, understanding what they do to protect their environment. We learn from that. They then send their leaders into our environment to learn from that. There are a lot of opportunities for governments who collaborate closely with industry players, and I think the U.S. does that fairly well.

The Chair: That's a key takeaway. Thank you very much. That's helpful.

Mr. Smith: I don't think I can add anything to that. That was pretty comprehensive.

[Translation]

Senator Dagenais: My question goes to all three witnesses. Do you know how the perpetrators of cyber attacks are able to develop tools to successfully carry out these attacks? Who gives them these tools?

De plus, nous avons récemment autorisé le recours à des mesures disciplinaires progressives contre les personnes qui cliquent à répétition sur des liens malveillants et qui infectent des machines dans notre milieu, ce qui peut mener au congédiement. Après trois prises, c'est le renvoi.

Le président : J'ai quelques brèves questions avant de passer au deuxième tour, si je peux me permettre. Je suis curieux de savoir si l'un de vous peut m'indiquer un pays qui a maintenant recours à des pratiques exemplaires pour gérer ce genre de problèmes.

M. Gordon : La situation peut être abordée de différentes façons. Il ne fait aucun doute que certains pays ont investi des sommes considérables dans la mise au point de technologies. Israël est un bon exemple de pays qui incube les petites entreprises qui sont nouvelles dans le secteur cybernétique. Pour ce qui est des normes, les États-Unis sont le chef de file mondial grâce au National Institute for Standards qui offre d'excellents produits et de bons conseils. En fait, le Canada adopte beaucoup des mêmes pratiques. Le Royaume-Uni fait quant à lui un travail intéressant en fusionnant ce qui est offert par le gouvernement avec certaines normes de travail destinées aux PME. C'est un mélange. Vous devriez adopter les pratiques exemplaires de plusieurs de ces pays. Je crois que les trois que j'ai mentionnés sont très bons.

M. Green : Les pratiques des pays dont Robert a parlé sont des choses auxquelles je réfléchis. Je crois que ce qui est le plus utile pour moi à titre de protecteur d'une organisation, ce sont les collaborations entre le gouvernement et l'industrie. Je suis d'avis que, aux États-Unis, dans le cadre de partenariats comme le FS-ISAC ou lorsque le gouvernement est un acteur important, nous avons beaucoup à apporter en tant qu'entreprises distinctes. Cela nous permet de prendre des mesures comme l'envoi de dirigeants de mon équipe dans une autre entreprise. À titre d'exemple, Canadian Tire est membre du FS-ISAC. Nous y envoyons nos dirigeants pour qu'ils comprennent ce que l'entreprise fait pour se protéger. Nous en tirons des leçons. Canadian Tire nous envoie ensuite ses dirigeants pour qu'ils apprennent de notre milieu. De nombreuses occasions s'offrent aux gouvernements qui collaborent étroitement avec des intervenants de l'industrie, et je pense que les États-Unis le font assez bien.

Le président : C'est un point essentiel à retenir. Merci beaucoup. C'est utile.

M. Smith : Je ne pense pas avoir quelque chose à ajouter. C'était détaillé.

[Français]

Le sénateur Dagenais : Ma question s'adresse aux trois témoins. Savez-vous comment les auteurs de cyberattaque réussissent à élaborer des outils pour réussir une cyberattaque et, le cas échéant, qui leur fournit ces outils?

[English]

Mr. Green: They create tools a number of ways. If you look at recent attacks, they leverage things that have been stolen even from nation states. The WannaCry, Petya and NotPetya outbreaks leverage technology stolen from the NSA. Just like we have corporations and companies that come up with new and innovative ways to do things, there are groups who work collectively to create new and innovative ways to take advantage of things. Any time there's a vulnerability that's discovered, there's a period of time that we, as a company, have to mitigate that vulnerability before bad guys work, come up with a means to exploit that at scale, and then try to inflict that on us.

Mr. Gordon: The short answer is it's become a business now. The cyber attackers are learning from one another. They're sharing attack techniques back and forth. If they're successful in attacking one company, they will send that along to everyone else. It's become a very good industry for them. As Mr. Green was saying, perfecting this is a business model.

Mr. Smith: The last thing I could add — and it was raised earlier — is the weakest link tends to be the pathway to get to the biggest prize. The value chain, where the smallest companies don't necessarily have the provisions in place to prevent or recognize those attacks have happened and have some kind of actionable intelligence, they end up going through those pathways to the larger companies where they're network connected. That's one of the things we need to deal with.

Senator Wetston: I'd like to use the sports analogy here. I see cybersecurity being all about defence. Any offence?

Mr. Smith: There are tools in the chest governments have access to and the Government of Canada now has access to. The Anti-terrorism Act, for instance, that was brought in in 2015 — most people know it as Bill C-51 — provides the opportunity for the RCMP or CSEC to engage in an offensive way on cybercriminals, where they're actually infecting the criminals. Maybe that's something we should take better advantage of.

Mr. Gordon: In the legislation that's currently before Parliament, expanding the powers of CSE in the offensive capability. That would give them the authority to actually undertake some of those operations.

Mr. Green: You're right. It's a defensive game. We have to be right all of the time. They only have to be right once. There is an opportunity to work with governments to figure out or delineate where that line is to go offensive. We won't go on the offensive, but working with government agencies, they could go on the offensive to protect what it is that we have.

[Traduction]

M. Green : Ils procèdent de différentes façons. Dans le cas des attaques menées récemment, les pirates ont même utilisé des outils qu'ils avaient volés à des États-nations. Les pannes causées par WannaCry, Petya et NotPetya passent par une technologie volée à la NSA. À l'instar des sociétés et entreprises qui créent des outils innovateurs pour accomplir certaines choses, différents groupes travaillent de concert pour créer des outils innovateurs pour exploiter le système. Quand une entreprise décele une vulnérabilité, elle dispose d'un certain laps de temps pour atténuer les risques avant que les pirates ne trouvent un moyen d'exploiter la faille à grande échelle, et qu'ils tentent une attaque.

M. Gordon : En bref, la réponse est que c'est devenu une industrie. Les auteurs de cyberattaques apprennent les uns des autres. Ils s'échangent des techniques sans arrêt. S'ils réussissent à attaquer une entreprise, ils envoient leur truc à tous les autres pirates. C'est devenu une véritable industrie. Comme M. Green le mentionnait, perfectionner leurs outils est leur nouveau modèle d'affaires.

M. Smith : Il en a été question plus tôt, mais j'ajouterais simplement que le maillon le plus faible semble être le chemin à suivre pour atteindre la cible la plus intéressante. Les pirates suivent la chaîne de valeur, en visant d'abord les petites entreprises qui n'ont pas les moyens de prévenir ni de reconnaître ces attaques. Ils obtiennent ainsi des renseignements qui leur permettent d'exploiter les connexions réseau et d'atteindre les grandes entreprises. C'est une des réalités avec lesquelles nous devons composer.

Le sénateur Wetston : J'aimerais y aller d'une analogie sportive. On dirait que la cybersécurité joue uniquement en zone défensive. Qu'en est-il de l'offensive?

M. Smith : Les gouvernements ont accès à différents outils, et le gouvernement du Canada ne fait pas exception. Par exemple, la Loi antiterroriste, surtout connue comme le projet de loi C-51 et adoptée en 2015, permet à la GRC et au CSTC de passer à l'offensive face aux cybercriminels, en les infectant eux-mêmes d'un virus. C'est peut-être un outil dont nous devrions nous servir davantage.

M. Gordon : Le projet de loi à l'étude devant le Parlement permettrait d'élargir les pouvoirs du CST à cet égard. Il serait ainsi autorisé à agir de manière offensive.

M. Green : Vous avez raison, la cybersécurité se joue en zone défensive. Nous devons bloquer tous les tirs, alors que les pirates n'ont qu'à marquer une seule fois. Il serait possible de travailler avec les gouvernements pour déterminer où se situe la limite acceptable pour les mesures offensives. Nous ne passerons pas à l'offensive, mais les entités gouvernementales pourraient le faire pour protéger nos avoirs.

Senator Wetston: This question is about cross-border activity. You're global. We have a lot of cross-border activity in all aspects of our business and financial markets. Are we weaker than the U.S. in cybersecurity? I'm putting you on a limb here. It's not about fairness, right?

Mr. Green: I've grown up in the U.S. and I've been in the financial sector for a long time. It suffered so much in the way of attacks that it was forced to Darwinism; it was forced to adapt earlier.

Senator Wetston: I don't mean to be unfair, but just give us a sense of it. I don't want to put you on the spot.

The Chair: Now that you have.

Senator Wetston: In a cross-border environment, it would be helpful if we were on the same page or close to having the same capabilities. For MasterCard, which is a global company that does a lot of business, for example, in Canada-U.S. in cross-border transactions, you probably hope for that, I would think.

Mr. Green: There are a lot of advantages to the interconnectedness. Our ability to see the transactions worldwide gives us an ability to protect things that aren't even in the U.S. For example, with our safety net we can see when an adversary, a hacker, has taken over a processor and is about to launch large cash-out gains. We can see that because we can see it across the globe. Our interconnectedness gives us an advantage to help our customers globally, no matter if they be in Canada, or Africa, or things of that nature.

The Chair: Well handled, Mr. Green.

Gentlemen, that was extremely helpful. You obviously did a lot of preparation to bring you here today and we very much appreciate that, because we've taken very good notes of what you've said, so thank you very much.

It is my privilege and pleasure to welcome individuals from the International Monetary Fund to brief the Standing Senate Committee on Banking, Trade and Commerce. I have the privilege of welcoming Cheng Hoon Lim, Assistant Director and Mission Chief for Canada, Western Hemisphere Department, International Monetary Fund; and as well, Troy Matheson, Senior Economist and Kotaro Ishi, Senior Economist.

We have had the opportunity to review your recent review on Canada and we're very interested to hear your comments today, and don't pull any punches.

The floor is yours.

Le sénateur Wetston : Ma prochaine question porte sur les activités transfrontalières. Vous êtes partout dans le monde. Nos marchés commerciaux et financiers donnent lieu à une multitude de transactions transfrontalières. Est-ce que la cybersécurité au Canada est moins rigoureuse qu'aux États-Unis? Je vous mets sur la sellette, mais ce n'est pas dans le but de mettre votre loyauté à l'épreuve.

M. Green : J'ai grandi aux États-Unis et je travaille dans le secteur financier depuis longtemps. Le secteur financier a subi tellement d'attaques qu'il n'a eu d'autre choix que de s'adapter rapidement; c'est la sélection naturelle à l'œuvre.

Le sénateur Wetston : Je ne veux pas vous mettre dans l'embarras, mais pourriez-vous nous donner une petite idée?

Le président : Vous l'avez déjà fait.

Le sénateur Wetston : Dans un contexte transfrontalier, ce serait utile si nous pouvions être sur la même longueur d'onde ou avoir à peu près la même capacité. Pour MasterCard, une société internationale qui traite de nombreuses transactions transfrontalières entre le Canada et les États-Unis, entre autres, j'imagine que ce serait souhaitable.

M. Green : L'interconnectivité offre de nombreux avantages. Étant en mesure de voir les transactions effectuées à l'échelle internationale, nous pouvons protéger des choses qui ne sont même pas aux États-Unis. Par exemple, notre filet de sécurité nous avertit lorsqu'un pirate a pris le contrôle d'un processeur et qu'il s'apprête à encaisser d'importantes sommes. Nous pouvons intercepter de telles commandes, car nous voyons ce qui se passe partout dans le monde. Cette interconnectivité nous aide à protéger nos clients, qu'ils soient au Canada, en Afrique ou ailleurs.

Le président : Bien répondu, monsieur Green.

Messieurs, vos témoignages ont été extrêmement utiles. De toute évidence, vous êtes arrivés fin prêts à la séance d'aujourd'hui, et nous vous en sommes très reconnaissants. Nous avons pris bonne note de vos commentaires. Merci beaucoup.

J'ai le privilège et le plaisir d'accueillir des représentants du Fonds monétaire international, qui répondront aux questions du Comité sénatorial permanent des banques et du commerce. Souhaitons la bienvenue à Cheng Hoon Lim, sous-directrice et chef de mission pour le Canada, Département hémisphère occidental, Fonds monétaire international, ainsi qu'à Troy Matheson et Kotaro Ishi, tous deux économistes principaux.

Nous avons eu la chance d'étudier votre dernier rapport sur le Canada, et nous sommes très intéressés à entendre vos commentaires. N'ayez pas peur de nous donner l'heure juste.

La parole est à vous.

Cheng Hoon Lim, Assistant Director and Mission Chief for Canada, Western Hemisphere Department, International Monetary Fund: We are delighted to be here this morning to present the IMF's view on Canada's growth outlook for 2018-19. Before I jump ahead to that assessment, I think it will be useful to start with a brief recap of what happened in 2017 in terms of economic developments.

The final fourth-quarter data will be released tomorrow but we expect the economy ended 2017 on a high note, with Canada posting a growth rate of almost 3 per cent, the highest among G7 economies. Now the first half of 2017 was stronger than the second half but overall, the positive outcome reflected the confluence of expansionary, fiscal and monetary policies, a strong U.S. economy and stable oil prices.

Private consumption continues to be the main driver of growth. Now we expect the growth momentum to slow in 2018-19 as policy levers tighten. We project GDP growth to moderate to 2.3 per cent in 2018 and 2 per cent in 2019. At these levels, the economy will still be growing above capacity. An important reason is our assumption on U.S. growth. Now, this is important to our baseline projection and we assume the cut in U.S. corporate taxes from 35 per cent to 21 per cent, with immediate expensing of investment, will have a positive demand effect on Canada. The U.S. economy will grow faster and this will increase the demand for Canadian exports and narrow the current deficit. Overall, we expect the U.S. tax cut to contribute roughly 0.3 percentage points to Canadian growth, over 2018-19.

The second important assumption underlying our baseline projection is investment.

Here, we expect non-residential investment to recover. As you know, investment had declined for two consecutive years in 2015-16. Last year was the first year in which business investment resumed. We expect this to gradually recover and the reason we think the recovery would be more gradual is because of uncertainty related to NAFTA and the fact interest rates are likely going to increase over the course of the next two years.

The third assumption underlying our projection is on oil exports. We expect that to remain fairly constant as a share of GDP over the projection horizon. We assume oil prices will fall somewhere in the range of \$50 and \$60 per barrel, and pipeline and other supply constraints do not significantly impact the spread between the Canadian Western Select price and the global benchmark, WTI. We expect investment in the oil sector next year to remain flat.

Cheng Hoon Lim, sous-directrice et chef de mission pour le Canada, Département hémisphère occidentale, Fonds monétaire international: Nous sommes ravis d'être ici ce matin pour vous présenter le point de vue du FMI en ce qui a trait aux perspectives de croissance du Canada pour 2018-2019. Avant d'entrer dans le vif du sujet, je crois qu'il serait utile de récapituler brièvement les développements économiques de 2017.

Les données du quatrième et dernier trimestre de 2017 seront rendues publiques demain, mais nous nous attendons à une clôture positive, puisque le Canada a enregistré un taux de croissance de près de 3 p. 100, se positionnant ainsi en tête des pays du G7. Le premier semestre de 2017 a été supérieur au deuxième, mais globalement, la confluence des politiques expansionnistes, fiscales et monétaires, de la solidité de l'économie américaine et de la stabilité des prix du pétrole a donné lieu à des résultats positifs.

La consommation privée continue d'être le principal moteur de la croissance. Cet élan devrait ralentir en 2018-2019 avec le resserrement des leviers politiques. Nous projetons un ralentissement de la croissance du PIB, qui devrait passer à 2,3 p. 100 en 2018, et à 2 p. 100 en 2019. Encore là, la croissance économique surpassera la capacité. Nos projections se basent en grande partie sur la croissance présumée de l'économie américaine. Notre hypothèse veut que la baisse de l'impôt des sociétés aux États-Unis, qui passera de 35 à 21 p. 100, et la passation en charges immédiate des investissements, auront un effet positif sur la demande au Canada. L'économie américaine connaîtra une croissance accrue, ce qui aura pour effet d'augmenter la demande en exportations canadiennes et réduire le déficit actuel. Dans l'ensemble, nous prévoyons que la réduction fiscale des États-Unis contribuera à une hausse de 0,3 p. 100 de la croissance canadienne en 2018-2019.

La deuxième grande hypothèse soutenant nos prévisions de base concerne les investissements.

Nous prévoyons une reprise des investissements non résidentiels. Comme vous le savez, les investissements avaient connu une baisse pendant deux années consécutives, soit en 2015-2016. Le placement d'entreprise a repris pour la première fois l'an dernier depuis cette période. Nous prévoyons une reprise graduelle des investissements, et cette reprise pourrait être ralentie par l'incertitude entourant l'ALENA et la hausse probable des taux d'intérêt au cours des deux prochaines années.

Notre troisième hypothèse porte sur les exportations pétrolières. Nous prévoyons qu'elles représenteront une part assez constante du PIB au cours de la période projetée. Nous présumons que le prix du baril de pétrole se situera entre 50 et 60 \$, et les contraintes associées aux pipelines et aux autres modes d'approvisionnement ne devraient pas avoir une grande incidence sur l'écart entre le prix du Western Canadian Select et le prix de référence mondial. Nous prévoyons que les

Fourth, we expect interest rates to rise in response to inflation pressures. This will slow consumer spending as debt service costs rise. Similarly, we expect higher interest rates with tight macroprudential policies to dampen residential investment.

Last, we assume fiscal policy will remain broadly neutral, with the federal deficit at around less than 1 per cent of GDP.

So this is essentially the gist of our baseline projection for 2018 and 2019. As you can see, in the near term, prospects are bright primarily because of a very strong U.S. economy with positive demand spillovers to Canada.

That being said, there is considerable uncertainty around the outlook, particularly with regard to assumptions on NAFTA, the U.S. tax reform, household debt and the housing market. Let me briefly go through these three potential sources of uncertainty to our outlook.

As you know, the seventh round of NAFTA negotiations is ongoing in Mexico City. Although there has been significant progress in modernizing NAFTA by including developments in digital and e-commerce, several proposals put forward by the U.S. such as minimum U.S. content requirements in the auto sector, eliminating the dispute resolution framework, placing a cap on government procurement and introducing a five-year sunset clause represent major points of contention for the negotiations.

So uncertainty related to NAFTA, whether it's going to be a good or bad outcome, is already affecting investor sentiment in Canada, and failure to forge a new agreement or have at least as good an outcome as we have today, could impact investment for a much more prolonged period. To summarize what I've just said, there's a downside risk to our projection on investment.

There's a further source of uncertainty on investment, and that comes from the U.S. tax reform.

While we anticipate the U.S. tax reform will boost the U.S. economy and that will have positive spillovers to Canada from a demand perspective — they will buy more Canadian goods and services — what we have not taken into account in our outlook is there is a possibility certain aspects of the tax reform that go beyond just the tax cuts, there are other aspects that could result

investissements dans le secteur pétrolier resteront au même niveau au cours de la prochaine année.

Quatrièmement, nous nous attendons à une hausse des taux d'intérêt en réaction à la pression inflationniste. Cela entraînera un ralentissement des dépenses de consommation, parallèlement à une hausse des frais de service de la dette. De la même façon, nous prévoyons que la hausse des taux d'intérêt, combinée à des politiques macroprudentielles strictes, pourrait freiner les investissements résidentiels.

Et finalement, nous présumons que les politiques fiscales resteront généralement neutres, le déficit fédéral s'élevant à moins de 1 p. 100 du PIB.

Voilà donc essentiellement nos prévisions de base pour 2018 et 2019. Comme vous pouvez le constater, à court terme, les perspectives sont encourageantes, principalement en raison de la forte économie américaine, qui aura des retombées positives pour la demande au Canada.

Cela dit, une grande incertitude plane, notamment pour les hypothèses concernant l'ALENA, la réforme fiscale américaine, l'endettement des ménages et le marché de l'habitation. Permettez-moi de passer en revue ces trois sources potentielles d'incertitude.

Vous le savez, le septième cycle de négociations de l'ALENA est en cours à Mexico. Bien que d'importants progrès aient été faits en vue de la modernisation de l'ALENA, entre autres par l'inclusion du commerce numérique et électronique, plusieurs dispositions proposées par les États-Unis sont sources de litiges importants dans les négociations. Je note par exemple les exigences relatives au contenu américain obligatoire dans le secteur automobile, l'élimination du cadre de règlement des conflits, l'imposition d'un plafond sur l'approvisionnement public, et l'instauration d'une clause de temporisation de cinq ans.

Donc, le climat d'incertitude entourant l'ALENA, que l'issue soit positive ou négative, influe déjà sur l'opinion des investisseurs au Canada. En l'absence d'une nouvelle entente, ou à tout le moins d'avoir un résultat un tant soit peu positif comme nous le voyons aujourd'hui, l'investissement pourrait s'en ressentir pendant une assez longue période. En résumé, nos projections en matière d'investissement comportent des risques baissiers.

Un autre facteur contribue à l'incertitude liée à l'investissement, et c'est la réforme fiscale des États-Unis.

Nous nous attendons à ce que la réforme fiscale des États-Unis vienne stimuler l'économie américaine et qu'elle ait des retombées positives pour la demande au Canada, puisque les Américains achèteront plus de biens et de services canadiens. Cependant, il est possible que cette réforme prévoie des mesures allant au-delà des simples baisses d'impôt, et qu'elle profite aux

in profit or production shifting away from Canada and to the U.S.

These effects are extremely difficult to estimate, but if the net effect of these changes leave Canada less competitive as an investment destination, then we could see an outflow of investment from Canada to the U.S. So this is another downside risk to our investment forecast.

Finally, as I said earlier, consumption has really been the primary engine of growth for the Canadian economy for the past few years. We have seen business investment quite lacklustre, and non-energy exports have not increased to the extent we would have expected, given a depreciation in the Canadian dollar.

So private consumption and residential investment are the main contributors in our growth outlook for 2018-19, and they are a function of the state of the housing market. With household debt continuing to rise — and I think we've seen household debt to income rising by 3 percentage points just in 2017 alone; it has now gone up to 173 per cent of disposable income — households become more vulnerable to unemployment or interest rate shocks. So a sharp correction in house prices will reduce housing growth, reduce consumer confidence, raise borrowing costs and lead to lower consumer spending and lower residential investment activity.

If the housing market correction is accompanied by a severe recession, bank balance sheets could be impaired, triggering negative feedback loops in the economy.

This presents another downside risk to our assumption in our growth outlook for 2018-19. The good news is macroprudential policies are beginning to bite and slow down real estate activity, but a significant decline in vulnerability may take several years because of the large stock of outstanding debt.

Let me stop here. We're happy to take any questions from senators.

The Chair: Thank you very much. A tremendous overview.

Senator Tkachuk: I just have a few questions on household debt in Canada. There seems to be some concern by your organization about Canada's household debt. I have a couple of questions on that.

Is household debt mostly driven by real estate or is it driven by the purchase of other commodities?

États-Unis au détriment du Canada, qui pourrait perdre une part des profits et de la production. Et nos projections ne tiennent pas compte de ce facteur.

Il est extrêmement difficile d'évaluer de tels effets, mais, si ces changements viennent entraver la compétitivité du Canada, on pourrait assister à un exode d'investisseurs vers les États-Unis. C'est donc un autre risque baissier à prendre en compte à cet égard.

Finalement, comme je le disais tout à l'heure, la consommation est véritablement la principale force motrice de la croissance économique du Canada depuis quelques années. Les placements d'entreprise sont peu reluisants, et les exportations de produits non énergétiques n'ont pas connu la hausse attendue, compte tenu de la dépréciation du dollar canadien.

La consommation privée et les investissements résidentiels sont ainsi les principales sources de croissance pour nos perspectives de 2018-2019, et ces deux éléments sont déterminés par l'état du marché de l'habitation. L'endettement des ménages étant toujours à la hausse — et je crois qu'il a gagné trois points de pourcentage en 2017 seulement, pour atteindre 173 p. 100 du revenu disponible —, les ménages sont davantage vulnérables au chômage ou à la hausse soudaine des taux d'intérêt. Une correction drastique du prix des maisons va ainsi freiner la croissance du marché de l'habitation, miner la confiance du consommateur, entraîner la hausse des coûts d'emprunt, de même que ralentir les dépenses de consommation et les investissements résidentiels.

Si la correction du marché de l'habitation s'accompagne d'une grave récession, le bilan des banques pourrait s'en trouver affaibli, entraînant un cercle vicieux néfaste pour l'économie.

Cela représente un autre risque de baisse dans nos perspectives de croissance pour 2018-2019. La bonne nouvelle est que les politiques macroprudentielles commencent à faire effet et à ralentir l'activité immobilière. Toutefois, il faudra peut-être attendre plusieurs années avant de voir une atténuation importante des vulnérabilités, vu l'ampleur de l'endettement.

Je m'arrête ici. Nous serons heureux de répondre aux questions des sénateurs.

Le président : Merci beaucoup. C'est un excellent tour d'horizon.

Le sénateur Tkachuk : J'ai simplement quelques questions sur la dette des ménages au Canada, un enjeu qui semble préoccuper votre organisation. J'ai quelques questions à ce sujet.

Est-ce que la dette des ménages repose principalement sur l'immobilier ou sur d'autres produits?

Ms. Lim: It is mainly real estate. Eighty per cent of household debt is essentially mortgage debt and home equity lines of credit, which are lines of credit that households draw on to withdraw equity from the value of houses to spend on education, durable goods and so on. So those two combined make up most of the household debt. It's related to housing.

Senator Tkachuk: How is that affecting savings rates for Canadians?

Ms. Lim: It has declined to about 4 and a half per cent.

Senator Tkachuk: Is that above normal or normal? Do you think that's too high or too low?

Ms. Lim: Compared to what we have seen in Canada in the past, it is low.

Senator Tkachuk: Is the debt driven by optimism or is it driven by lack of cash?

Ms. Lim: That's an interesting question. I don't think —

Senator Tkachuk: It's the only question, actually.

Ms. Lim: I think in some respects it's driven by optimism. Households see house prices going up, so they basically want to get into the game, so to speak. They think if they don't get into the housing market today, they won't be able to afford houses in the future.

So given the fact interest rates are so low and have been for the last 10 years, in some sense it is rational for Canadian households to buy property. It has been cheap. Even though the average mortgage has increased in value because house prices have gone up in value, the debt servicing costs, if you look at a chart, have actually declined because interest rates have been so low. More Canadian households can afford more expensive properties because of the low interest rates.

Now, the risk, as I said earlier, is that the high household debt makes the average Canadian household more vulnerable to an unemployment shock or to an interest rate shock. If U.S. long-term bond yields go up, for example, that will spill over because Canadian long-term yields are closely tied to U.S. bond yields. With the U.S. economy growing at a much faster rate — they are expanding beyond maximum capacity — that could lead to increases in interest rates in the U.S. and could spill over to Canadian interest rates. So if mortgage rates were to increase, this would change the equation on the debt servicing capacity for Canadian households.

Mme Lim: Elle repose principalement sur l'immobilier. Quatre-vingts pour cent de la dette des ménages est composée essentiellement de la dette hypothécaire et de la marge de crédit hypothécaire — une marge de crédit qu'ils utilisent pour obtenir des capitaux sur la valeur de leur maison afin de payer les études des enfants, d'acheter des biens durables, et cetera. Ces deux éléments constituent le gros de la dette des ménages, et c'est donc lié au logement.

Le sénateur Tkachuk: Quelles répercussions cela a-t-il sur les taux d'épargne des Canadiens?

Mme Lim: Il a diminué à environ 4 p. 100 et demi.

Le sénateur Tkachuk: Est-ce normal ou supérieur à la normale? Croyez-vous que c'est trop élevé, ou trop bas?

Mme Lim: Comparativement à ce que nous avons observé par le passé au Canada, c'est bas.

Le sénateur Tkachuk: La dette est-elle stimulée par l'optimisme ou par le manque d'argent?

Mme Lim: C'est une question intéressante. Je ne pense pas...

Le sénateur Tkachuk: C'est la seule question, en fait.

Mme Lim: Je pense que, d'un certain point de vue, elle est stimulée par l'optimisme. Les ménages voient le prix des maisons augmenter, alors ils veulent être de la partie, si on veut. Ils ont l'impression que s'ils n'achètent pas une maison maintenant, ils n'auront pas les moyens de le faire plus tard.

Comme les taux d'intérêt sont très bas, et qu'ils l'ont été depuis les 10 dernières années, c'est logique en un sens que les ménages canadiens veuillent s'acheter une maison. C'est bon marché. Même si la valeur de l'hypothèque moyenne a augmenté en raison de l'augmentation du prix des maisons, le coût du service de la dette, si on regarde un tableau, a diminué en fait parce que les taux d'intérêt sont très bas. Les ménages canadiens sont plus nombreux à pouvoir s'acheter une maison qui coûte très cher en raison des faibles taux d'intérêt.

Le risque, comme je l'ai mentionné un peu plus tôt, est que l'endettement élevé du ménage moyen le rende plus vulnérable à une hausse subite du chômage ou des taux d'intérêt. Si le taux des obligations à long terme des États-Unis augmente, par exemple, l'effet se fera sentir au Canada, car les rendements au Canada et aux États-Unis sont intimement liés. L'économie américaine croît à un rythme beaucoup plus rapide maintenant — supérieur à la capacité maximale —, ce qui pourrait provoquer une hausse des taux d'intérêt et avoir un effet d'entraînement au Canada. Si les taux d'intérêt des prêts hypothécaires augmentent, cela aura un effet sur la capacité des ménages canadiens à les rembourser.

Senator Tkachuk: So when the Bank of Canada comes to visit us here and they issue their report and tell us about how they are concerned about the household debt of Canadians, they're really stimulating household debt by their monetary easing policy, which has been sort of the way for America and Canada to try to solve the problem of the market crash in 2008. They're actually stimulating consumers. They're enticing them to incur more debt because their interest rates are so low, lower than market.

Ms. Lim: Yes, and we've seen that not just in Canada but everywhere in the world. That is an appropriate response to unprecedented prices in 2008, when economies around the world, particularly the advanced world, were going into recession. So the right response would be to lower interest rates to stimulate the economy.

Now, in terms of household debt and housing risk, the IMF recommends macroprudential policies as a way to deal with vulnerability from the housing sector. Interest rate policy is to take care of the economy, and macroprudential policy is to take care of financial sector risks that might come from an overextended housing market.

Senator Tkachuk: All I'm saying is governments have tried to fix the problem with monetary easing. As you say, it was the right response, but sooner or later that response has to end. You can't continue pumping the money out and then all of a sudden worry about the housing crash that's going to happen because you're forcing the housing crash to happen. That's what governments are doing.

Ms. Lim: I think the process has already started. You have seen the Bank of Canada raising the policy rate twice last year because the economy grew by a lot last year. As the economy gains strength, you will see interest rates continuing to rise.

Yes, you're right. I think as they do that, the incentive to borrow will be reduced.

Senator Tkachuk: Thank you.

Senator Stewart Olsen: Thank you very much for appearing before us. I don't see as rosy a forecast as perhaps the IMF. I see the downsides as being perhaps a bit more gloomy.

In your report you released summer, you raised concerns about individual Canadian debt levels. You said it was mostly mortgage but as well government and business.

Le sénateur Tkachuk : Done, lorsque les représentants de la Banque du Canada viennent témoigner pour nous présenter leur rapport et nous faire part de leurs inquiétudes au sujet de la dette des ménages canadiens, cela veut dire en fait qu'en assouplissant la politique monétaire, ils ont stimulé l'endettement des ménages, et c'est un peu la solution qu'ont trouvée les États-Unis et le Canada pour remédier à l'effondrement du marché en 2008. On encourage la consommation. On encourage les consommateurs à s'endetter en leur offrant des taux d'intérêt très bas, plus bas que le marché.

Mme Lim : Oui, et c'est ce qui s'est produit pas seulement au Canada, mais partout dans le monde. C'est une mesure qui s'imposait pour contrer des prix sans précédent en 2008, quand des économies partout dans le monde, en particulier dans les pays industrialisés, sont entrées en récession. La stratégie la plus appropriée consiste à diminuer les taux d'intérêt pour stimuler l'économie.

En ce qui a trait maintenant à l'endettement des ménages et aux risques, le FMI recommande l'adoption de politiques macroprudentielles pour réduire la vulnérabilité du secteur de l'habitation. Les politiques liées aux taux d'intérêt visent à remédier à des problèmes économiques, tandis que les politiques macroprudentielles visent à atténuer les risques dans le secteur financier qui découlent d'une surchauffe du marché de l'habitation.

Le sénateur Tkachuk : Tout ce que je dis, c'est que les gouvernements ont tenté de régler le problème par l'assouplissement monétaire. Comme vous l'avez mentionné, c'était la chose à faire, mais, tôt ou tard, il faut y mettre fin. On ne peut pas continuer à stimuler l'économie, puis tout à coup, s'inquiéter de l'effondrement du marché immobilier qu'on a provoqué. C'est ce que les gouvernements font à l'heure actuelle.

Mme Lim : Je pense que le processus est déjà en cours. On a vu la Banque du Canada relever ses taux d'intérêt à deux reprises l'an dernier, en raison de la forte croissance économique. Plus l'économie prendra de la vigueur, plus on verra les taux d'intérêt augmenter.

Oui, vous avez raison. Je pense que plus ils augmenteront les taux d'intérêt, moins les gens seront tentés d'emprunter.

Le sénateur Tkachuk : Merci.

La sénatrice Stewart Olsen : Merci beaucoup de comparaître devant le comité. Je ne vois pas les prévisions aussi roses que le FMI. Je suis un peu plus pessimiste quant au retour du balancier.

Dans votre rapport rendu public l'été dernier, vous disiez vous inquiéter du niveau d'endettement des Canadiens, principalement lié aux prêts hypothécaires, mais vous avez parlé également des gouvernements et des entreprises.

Are you still concerned with that? When you have debt levels such as we have with government — and I'm not 100 per cent sure with business — any changes that push that teeter over to the other side are going to be quite devastating. Do you still have concerns about those other debt levels and could you explain a little bit?

Ms. Lim: Sure. In the report last year, we were mainly concerned with household debt because we think that is the main macro-financial vulnerability for the Canadian economy. When you refer to other debt, I presume you're referring to the government debt.

At the federal level, the government has actually been very prudent. The debt level, which on a net basis is even lower than the gross debt of about 30 per cent of GDP, is extremely low compared to the benchmark we've seen in OECD countries or G7 countries. Our assessment last year essentially said there is some fiscal space for the government to spend more — to invest more in the economy in terms of infrastructure, education and training and to promote innovation. We are not concerned about the level of federal government debt.

I think at the general government level, the debt is bumping at about 90 per cent of GDP. There we would recommend — and we did so in our report last year — that the provinces with high debt levels do take measures to rein in spending and to put that debt on a downward path.

Senator Stewart Olsen: Following up on the provincial debt, my province is heavily in debt. Are you seeing a response to that report by the provinces to reduce their debt?

Ms. Lim: I believe that's a conversation we will have with them in the next consultation round. I think all provinces we have engaged with understand the problem. They are fully aware of the fiscal position they are in and they're also aware there are contingent liabilities that are not coming today, but maybe 10 or 20 years from now, from rising health care costs. I don't think we are preaching something they are not already aware of.

What we would emphasize is perhaps they consider more seriously some fiscal rules in order to inject more discipline in meeting fiscal targets.

Senator Tannas: Do you do anything with respect to per capita growth in the economy? Canada has fairly robust growth in population as a result primarily of immigration, but also I guess for getting the job done a little bit on our own, compared to other countries. Does the growth of the economy when you

Est-ce toujours une source d'inquiétudes pour vous? Quand les niveaux d'endettement de nos gouvernements sont aussi élevés — et je ne sais pas exactement ce qu'il en est des entreprises —, tout changement qui peut pousser le pendule à l'autre bout du balancier aura des effets dévastateurs. Est-ce que ces niveaux d'endettement vous inquiètent encore, et pouvez-vous nous en dire un peu plus à ce sujet?

Mme Lim : Bien sûr. Dans le rapport de l'an dernier, nous étions surtout préoccupés par l'endettement des ménages, car nous pensons que c'est là où se trouve la principale vulnérabilité macrofinancière de l'économie canadienne. Quand vous parlez des autres dettes, je présume que vous parlez de la dette des gouvernements.

Au fédéral, le gouvernement a agi, en fait, de manière très prudente. Le niveau d'endettement — la dette nette est même plus basse que la dette brute qui est à environ 30 p. 100 du PIB — est extrêmement bas comparativement aux autres pays de l'OCDE ou du G7. Notre évaluation de la situation l'an dernier disait essentiellement que le gouvernement disposait d'une certaine marge financière pour dépenser davantage, pour investir davantage dans l'infrastructure, l'éducation, la formation et l'innovation. Le niveau d'endettement du gouvernement fédéral n'est pas une source de préoccupations pour nous.

Je pense que, au pays dans l'ensemble, la dette des gouvernements a atteint environ 90 p. 100 du PIB. Nous recommandons donc — et c'est ce que nous avons fait dans notre rapport l'an dernier — que les gouvernements provinciaux qui ont des niveaux d'endettement élevés prennent des mesures pour juguler leurs dépenses et diminuer leur endettement.

La sénatrice Stewart Olsen : Au sujet de l'endettement des provinces, la mienne est très endettée. Est-ce que, dans la foulée de votre rapport, les provinces vous semblent en voie de réduire leur endettement?

Mme Lim : Je crois que c'est une conversation que nous aurons avec elles lors de nos prochaines consultations. Je pense que toutes les provinces avec qui nous avons discuté comprennent le problème. Elles sont tout à fait conscientes de la situation financière dans laquelle elles se trouvent et du passif éventuel qui ne se manifesterait pas aujourd'hui, mais dans 10 ou 20 ans, lorsque les coûts de la santé augmentent. Je n'ai pas l'impression que nous prêchons à propos d'une situation qu'elles ignorent.

Nous allons probablement leur recommander de mettre en place des règles budgétaires plus sévères pour atteindre leurs objectifs.

Le sénateur Tannas : Calculez-vous la croissance par habitant dans l'économie? Le Canada connaît une croissance assez robuste de sa population en raison principalement de l'immigration, mais aussi parce que nous y mettons un peu plus du nôtre que dans d'autres pays. Est-ce que la croissance de

normalize for population growth change the position of Canada in any way in terms of its ranking in growth in GDP amongst the G7?

Ms. Lim: Essentially, we looked at labour productivity and how labour productivity is affected by demographic changes. We don't do a ranking, but Canada, like most advanced economies, is facing an aging population. That's going to continue to weigh on labour productivity growth.

We think it will be important for Canada to invest long-term in education and training to attract skilled immigration in order to address this demographic gap.

That's the extent to which we've done our analysis.

Kotaro, do you want to add anything here?

Senator Tannas: As you look at the U.S. economy, and the extent that it's growing, are U.S. consumers leveraging up again? How much of that growth is as a result of rising household debt?

Ms. Lim: I think the U.S. economy had significantly delevered after the 2008 crisis. Although some parts of the housing markets have rebounded, we still don't see a releveraging in an alarming manner. The recovery we have seen in the U.S. has actually been a rebound of investment in the U.S.

Senator Wetston: I cannot take issue with your assessment, but I do have some discomfort, and have had for quite a while, with respect to the tools that you rely on for your assessment.

I have discussed this issue with other Canadian economists. While I have a great deal of comfort with microeconomics, recently I have more discomfort with macroeconomics and the economic tools and models you rely on. I want to ask a couple of general questions around that.

What's your track record like in forecasting GDP growth for Canada and the U.S. since the financial crisis? Are you bang on? Have you missed by 1, 2, per cent, half a per cent, which is a lot in an economy? Can you help me with that?

Ms. Lim: You know, we're terribly sensitive about that.

Senator Wetston: Don't be, please. There is nothing to be sensitive about.

l'économie normalisée en fonction de la croissance de la population change la position du Canada parmi les pays du G7 pour ce qui est de la croissance de son PIB?

Mme Lim : On regarde essentiellement la productivité de la main-d'œuvre et les effets des changements démographiques sur la productivité de la main-d'œuvre. Nous n'effectuons pas de classement, mais le Canada, comme la plupart des économies avancées, a une population vieillissante. C'est un facteur qui continuera de peser sur la croissance de la productivité de sa main-d'œuvre.

Selon nous, il sera important pour le Canada d'investir à long terme dans l'éducation et la formation pour attirer des immigrants qualifiés afin de combler le fossé démographique.

C'est là la portée de notre analyse.

Kotaro, aimeriez-vous ajouter quelque chose?

Le sénateur Tannas : Quand on regarde du côté des États-Unis et du rythme de croissance de leur économie, est-ce que les consommateurs américains stimulent l'économie à nouveau? Quelle part de la croissance est attribuable à l'augmentation de l'endettement des ménages?

Mme Lim : Je pense que l'économie américaine a beaucoup ralenti après la crise de 2008. Même si certains segments du marché de l'habitation ont connu un rebond, on n'observe pas une reprise inquiétante. La reprise aux États-Unis est attribuable, en fait, à une reprise des investissements au pays.

Le sénateur Wetston : Je ne peux pas remettre en question votre analyse, mais j'éprouve une certaine réticence, et cela, depuis un certain temps, à l'égard des outils que vous utilisez pour effectuer vos analyses.

J'ai discuté de la question avec d'autres économistes au Canada. Si je suis tout à fait à l'aise avec les outils microéconomiques que vous utilisez, je le suis moins dernièrement avec vos outils et vos modèles macroéconomiques et économiques. J'ai quelques questions générales à vous poser à ce sujet.

À quoi ont ressemblé vos prévisions de croissance du PIB du Canada et des États-Unis depuis la crise financière? Avez-vous visé juste? Y avait-il un écart de 1 p. 100, de 2 p. 100 ou de 0,5 p. 100, ce qui est beaucoup dans une économie? Pouvez-vous m'éclairer à ce sujet?

Mme Lim : Vous savez, nous sommes terriblement chatouilleux sur cette question.

Le sénateur Wetston : Ne le soyez pas, s'il vous plaît. Il n'y a pas de raison de l'être.

Ms. Lim: I think as a general point, you're right. Sometimes we economists tend to rely too much on fancy tools and models. But we realize that. We don't only rely on models and tools to make projections. We look at a lot of data, we talk to a lot of people and we study surveys before we come to projections.

Now, have we always hit the mark in our projections? No. There was a chart, but I can't remember the numbers off the top of my head — Troy might know. We had a chart that was shared which showed how the real world economic outlook projections for global growth was revised systemically revised downward, in each publication. So, yes, we have missed our projections. It could be up to 1 percentage point; I can't remember the exact numbers now. However, I think that is the nature of forecasting.

Senator Wetston: Sure, and I don't want to put you on the spot because, frankly, I have a lot of respect for the work of the IMF. Central banks and other financial institutions and many other institutions rely on similar models and data. I'm not suggesting that is the case, I'm just trying to understand it in the context of your assessment.

Since the financial crisis, I think you would all agree with me that globally — but I'll talk about Canada and maybe the U.S. a bit — we have been in uncharted territory. I don't think we've experienced a period of quantitative easing as long, nor have we experienced the impact the financial crisis had on the global economy.

Are we still in uncharted territory, from your perspective? Are you now able to say, based on some of the discussion today in your presentation, as well as the answer to the questions? My own personal belief is I still think we are somewhat in the area of uncharted territory, but that's just my personal view. I'm wondering what yours would be.

Ms. Lim: In some ways we're in new uncharted territory with U.S. fiscal stimulus happening at a time when the U.S. economy is operating at full capacity. I think that is a new uncharted territory. We're not really sure what's going to happen in terms of the impact of the tectonic change in the U.S. corporate taxation, the impact on investment and on consumption.

Senator Wetston: We understand the monetary policy tools you have at your disposal, and we've learned a lot in the financial crisis. We've learned a lot about when I think fiscal policy tools are necessary, mostly because monetary policy tools are no longer effective. Have we exhausted monetary policy

Mme Lim : Je pense que, dans l'ensemble, vous avez raison. Les économistes que nous sommes ont tendance à trop utiliser de modèles et d'outils compliqués. Mais nous en sommes conscients. Nous n'utilisons pas seulement des modèles et des outils pour effectuer nos prévisions. Nous examinons une foule de données, nous consultons une foule de gens, et nous examinons les résultats d'enquêtes avant d'effectuer nos prévisions.

Avons-nous toujours visé juste dans nos prévisions? Non. Nous avions un tableau, mais je ne me rappelle pas des données — Troy pourrait s'en souvenir. Nous avions un tableau que nous avons diffusé et qui montre comment les perspectives de croissance de l'économie mondiale ont été revues systématiquement à la baisse lors de chaque publication. Donc, oui nos prévisions ont raté la cible. Cela pouvait atteindre jusqu'à un point de pourcentage; je ne me souviens pas des chiffres exacts. Je pense toutefois que c'est la nature des prévisions.

Le sénateur Wetston : Bien sûr, et je ne voulais pas vous mettre dans l'embarras, car honnêtement, j'ai beaucoup de respect pour le travail qu'effectue le FMI. Les banques centrales, d'autres institutions financières et de nombreuses autres institutions utilisent des données et des modèles similaires. Je ne dis pas que c'est le cas, mais j'essaie simplement de comprendre cela dans le cadre de votre analyse.

Depuis la crise financière, je pense que vous seriez tous d'accord avec moi pour dire que nous avons été mondialement en territoire inconnu — et je parlerai un peu du Canada, et peut-être aussi des États-Unis. Je ne pense pas que nous ayons déjà connu une période aussi longue d'assouplissement quantitatif, non plus qu'une crise financière ayant eu de pareilles répercussions sur l'économie mondiale.

Sommes-nous encore en territoire inconnu, à votre avis? Êtes-vous en mesure de le dire, à partir des discussions aujourd'hui et des réponses aux questions? Personnellement, je pense que nous sommes encore en territoire inconnu, mais c'est seulement mon opinion personnelle. J'aimerais connaître la vôtre.

Mme Lim : Je dirais que, dans une certaine mesure, les stimulants économiques aux États-Unis, à un moment où l'économie américaine tourne à plein régime, nous placent en nouveau territoire inconnu. Je pense qu'on entre ici dans un nouveau territoire inconnu. Nous ne savons pas exactement quelles seront les répercussions des changements colossaux qu'ils ont apportés à l'imposition des entreprises, et quelles en seront les répercussions sur l'investissement et la consommation.

Le sénateur Wetston : Nous connaissons les outils de politique monétaire qui sont à votre disposition, et nous avons beaucoup appris de la crise financière. Nous avons beaucoup appris, je pense, sur l'utilisation nécessaire des outils de politique budgétaire, principalement lorsque les outils de

tools with respect to dealing with matters like the new uncharted territory that we're entering into?

Ms. Lim: One of the consequences of this uncharted territory, as you put it, is the fact we have pushed monetary policy beyond the zero lower bound. Some central banks in Europe and Japan have used negative interest rates as a policy tool, and Canada, as Troy pointed out, has negative real rates at the present time. We have the toolkit on quantitative easing that has provided a way for central banks to inject liquidity in an unprecedented way.

So all these suggest we haven't run out of tools per se; we have just become more creative about using them.

The Chair: I have two or three quick questions, if I may, please.

I think my notes must be wrong, but did you say that business investment into Canada will continue to recover?

Ms. Lim: Yes, in the sense they will recover from a low base. Business investment resumed in 2017. The investment figures we've seen for the first three quarters suggest a 7 per cent increase, I think, in business investment.

We're waiting for the final quarter data to be released tomorrow. My guess is investment numbers will be lower in the last quarter so the overall upturn for 2017 will be lower than the 7 per cent we saw in the first three quarters.

What we're saying is investment is going to continue to recover but, as I said, at a very gradual pace, because of the uncertainty surrounding NAFTA and the impact of other aspects of the U.S. tax reform.

The Chair: That's interesting, because anecdotally, in my conversations with investors and CEOs across Canada, particularly in the province of Alberta — my home province — I have the very clear sense that investment into Canada at this moment has stopped.

Ms. Lim: It's not looking good, yes. The FDI numbers came out this morning and show a decline in foreign direct investment. I think for Alberta in particular, investment in the oil and gas sector will probably be flat at best going into 2018.

The Chair: I'm encouraged only in that my notes weren't incorrect. Thank you very much.

politique monétaire ne sont plus efficaces. Avons-nous épuisé nos outils de politique monétaire pour traiter de situations comme ce nouveau territoire inconnu dans lequel nous nous apprêtons à entrer?

Mme Lim : Une des conséquences de ce territoire inconnu, comme vous l'appellez, découle du fait que nous avons poussé la politique monétaire au-delà du zéro. Certaines banques centrales en Europe et au Japon ont eu recours à des taux d'intérêt négatifs comme outil de politique, et le Canada, comme l'a mentionné Troy, a des taux réels négatifs à l'heure actuelle. Nous avons donc des outils d'assouplissement quantitatif qui ont permis aux banques centrales d'injecter des liquidités dans l'économie, de façon sans précédent.

Il semble donc que nous n'ayons pas épuisé nos outils à proprement parler; nous avons simplement fait preuve de plus d'ingéniosité dans leur utilisation.

Le président : J'ai deux ou trois petites questions, si je peux me permettre.

J'ai l'impression que mes notes ne sont pas exactes. Avez-vous dit que les investissements des entreprises au Canada poursuivront leur remontée?

Mme Lim : Oui, en ce sens qu'ils vont effectuer une remontée de leur bas niveau. Les investissements des entreprises ont repris en 2017. Les chiffres des trois premiers trimestres laissent entrevoir une hausse de 7 p. 100, si je me souviens bien.

Nous attendons les données du dernier trimestre qui seront publiées demain. J'ai l'impression que les investissements seront moindres au dernier trimestre, alors la remontée en 2017 sera en deçà des 7 p. 100 observés au cours des trois premiers trimestres.

Nous pensons que les investissements vont poursuivre leur remontée, mais, comme je l'ai mentionné, à un rythme graduel, en raison de l'incertitude qui entoure l'ALENA, et des répercussions d'autres aspects de la réforme fiscale aux États-Unis.

Le président : C'est intéressant, car, d'après les conversations que j'ai eues avec des investisseurs et des PDG partout au Canada, en particulier en Alberta — ma province d'origine —, j'ai la très nette impression que les investissements au Canada en ce moment sont au point mort.

Mme Lim : Les perspectives ne sont pas bonnes, oui. Les chiffres pour les IDE ont été publiés ce matin et révèlent une baisse des investissements directs étrangers. Si je me souviens bien, c'est le cas en particulier en Alberta, les investissements dans le secteur pétrolier et gazier demeureront stables, au mieux, au début de 2018.

Le président : La seule chose encourageante, c'est de voir que mes notes n'étaient pas erronées. Merci beaucoup.

What number are you forecasting to be the price differential per barrel of oil being exported from Canada in 2018?

Ms. Lim: We essentially take what's currently in the market, which is about a \$20 differential, and this has widened significantly.

The Chair: You bet.

My last question is: Are you able to offer any opinion as to what the effects on the Canadian economy would be in terms of our numbers for our potential growth in 2018-19 if there were a complete failure of NAFTA?

Ms. Lim: That's a tough one. We did some analysis last year where we looked at the impacts of Canada's going to MFN rates.

If NAFTA is abolished, and Mexico, Canada and the U.S. will have to trade with each other on the MFN tariff rates, we did some simple simulations that shows this will have a negative short-term impact on Canada's real GDP — the level of GDP — of about 0.4 per cent. But in the long term, consumption and investment will be lower by around 2 per cent, I believe. So there will be a negative impact.

The Chair: Thank you very much.

Are there any other questions around the table?

All that's left is for me to thank you all very much for doing the work you've done and making yourselves available today. I'm hoping you found this to be a pleasant experience, because we'd like to continue this on an annual basis, so you have a number of months to consider.

This was extraordinarily helpful in large part because you're looking at Canada from the outside in and you don't have a dog in the race, in that sense. We very much appreciate your insight.

We're indebted to you.

Ms. Lim: Thank you. It's been a pleasure.

(The committee adjourned.)

Quelles sont vos prévisions sur l'écart de prix du baril de pétrole canadien à l'exportation en 2018?

Mme Lim : Nous prenons essentiellement l'écart actuel sur le marché, qui est d'environ 20 \$ et qui a augmenté de façon significative.

Le président : C'est certain.

Ma dernière question est la suivante : seriez-vous en mesure de nous donner votre opinion sur les effets potentiels sur la croissance de l'économie canadienne, en 2018-2019, d'un échec total de l'ALENA?

Mme Lim : Vous posez là une question difficile. Nous avons réalisé une analyse l'an dernier dans laquelle nous avons examiné les répercussions pour le Canada de passer aux taux de la nation la plus favorisée.

Si l'ALENA est aboli, et que le Mexique, le Canada et les États-Unis doivent commercer aux taux de la nation la plus favorisée, les simulations simples que nous avons réalisées indiquaient que cela aurait des répercussions négatives à court terme sur le PIB réel du Canada — le pourcentage du PIB — d'environ 0,4 p. 100. Toutefois, à long terme, la consommation et les investissements diminueraient d'environ 2 p. 100, je crois. Il y aura donc des répercussions négatives.

Le président : Merci beaucoup.

Les sénateurs ont-ils d'autres questions?

Tout ce qu'il me reste donc à faire est de vous remercier sincèrement pour le travail que vous avez fait et votre disponibilité aujourd'hui. J'ose espérer que vous avez aimé l'expérience, car nous souhaiterions la répéter chaque année. Vous avez donc quelques mois pour y réfléchir.

La séance a été très utile pour nous, en particulier parce que vous avez un point de vue extérieur sur le Canada, et que vous n'avez pas de parti pris. Nous vous remercions de vos observations.

Nous vous sommes très reconnaissants.

Mme Lim : Merci. Ce fut un plaisir.

(La séance est levée.)

WITNESSES

Wednesday, February 28, 2018

Bank of Canada:

Ron Morrow, Managing Director, Financial Stability Department.

Department of Finance Canada:

Annette Ryan, Associate Assistant Deputy Minister, Financial Sector Policy Branch.

Office of the Superintendent of Financial Institutions Canada:

Judy Cameron, Senior Director, Legislation, Approvals and Strategic Policy;

Theresa Hinz, Director, Approvals and Precedents.

Payments Canada:

Justin Ferrabee, Chief Operating Officer;

Martin Kyle, Chief Information Security Officer.

Thursday, March 1, 2018

The Canadian Chamber of Commerce:

Scott Smith, Director, Intellectual Property and Innovation Policy.

Canadian Cyber Threat Exchange:

Robert W. Gordon, Executive Director.

MasterCard:

Ron Green, Chief Security Officer.

International Monetary Fund:

Cheng Hoon Lim, Assistant Director and Mission Chief for Canada, Western Hemisphere Department (by video conference);

Troy Matheson, Senior Economist (by video conference);

Kotaro Ishi, Senior Economist (by video conference).

TÉMOINS

Le mercredi 28 février 2018

Banque du Canada :

Ron Morrow, directeur général, Département de la Stabilité financière.

Ministère des Finances Canada :

Annette Ryan, sous-ministre adjointe déléguée, Direction de la politique du secteur financier.

Bureau du surintendant des institutions financières Canada :

Judy Cameron, directrice principale, Législation, approbations et politique stratégique;

Theresa Hinz, directrice, Approbations et précédents.

Paiements Canada :

Justin Ferrabee, chef des opérations;

Martin Kyle, dirigeant principal de la sécurité de l'information.

Le jeudi 1^{er} mars 2018

Chambre de commerce du Canada :

Scott Smith, directeur, Propriété intellectuelle et politique d'innovation.

Échange canadien de menaces cybernétiques :

Robert W. Gordon, directeur général.

MasterCard :

Ron Green, chef de la sécurité.

Fonds monétaire international :

Cheng Hoon Lim, sous-directrice et chef de mission pour le Canada, Département hémisphère occidental (par vidéoconférence);

Troy Matheson, économiste principal (par vidéoconférence);

Kotaro Ishi, économiste principal (par vidéoconférence).